Contents

Introduction to System Center Configuration Manager

5/23/2019 • 19 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

A product in the Microsoft System Center suite of management solutions, System Center Configuration Manager can help you manage devices and users both on-premises and in the cloud.

You can use Configuration Manager to help you:

- Increase IT productivity and efficiency by reducing manual tasks and letting you focus on high-value projects.
- Maximize hardware and software investments.
- Empower user productivity by providing the right software at the right time.

Configuration Manager helps you deliver more effective IT services by enabling:

- Secure and scalable software deployment.
- Compliance settings management.
- Comprehensive asset management of servers, desktops, laptops, and mobile devices.

Configuration Manager extends and works alongside your existing Microsoft technologies and solutions.

For example, Configuration Manager integrates with:

- Microsoft Intune to manage a wide variety of mobile device platforms.
- Windows Server Update Services (WSUS) to manage software updates.
- Certificate Services.
- Exchange Server and Exchange Online.
- Windows Group Policy.
- DNS.
- Windows Automated Deployment Kit (Windows ADK) and the User State Migration Tool (USMT).
- Windows Deployment Services (WDS).
- Remote Desktop and Remote Assistance.

Configuration Manager also uses:

- Active Directory Domain Services for security, service location, configuration, and to discover the users and devices that you want to manage.
- Microsoft SQL Server as a distributed change management database—and integrates with SQL Server Reporting Services (SSRS) to produce reports to monitor and track management activities.
- Site system roles that extend management functionality and use the web services of Internet Information Services (IIS).
- Background Intelligent Transfer Service (BITS) and BranchCache to help manage the available network bandwidth.

To be successful with Configuration Manager, you must first thoroughly plan and test the management features before you use Configuration Manager in a production environment. As a powerful management application, Configuration Manager has the potential to affect every computer in your organization. When you deploy and

manage Configuration Manager with careful planning and consideration of your business requirements, Configuration Manager can reduce your administrative overhead and total cost of ownership.

Use the following topics and additional sections in this topic to learn more about Configuration Manager.

Related topics in this documentation library:

- Features and capabilities of System Center Configuration Manager
- Choose a device management solution for System Center Configuration Manager
- What's changed in System Center Configuration Manager from System Center 2012 Configuration Manager
- Fundamentals of System Center Configuration Manager
- Evaluate System Center Configuration Manager by building your own lab environment
- Find help for using System Center Configuration Manager
- Removed and deprecated items for System Center Configuration Manager

The Configuration Manager console

After you install Configuration Manager, use the Configuration Manager console to configure sites and clients, and to run and monitor management tasks. This console is the main point of administration and lets you manage multiple sites.

You can use the console to run secondary consoles that provide support for specific client management tasks, like:

- **Resource Explorer**, to view hardware and software inventory information.
- **Remote control**, to remotely connect to a client computer to perform troubleshooting tasks.

You can install the Configuration Manager console on additional computers, and restrict access and limit what administrative users can see in the console by using Configuration Manager role-based administration.

For more information, see Install System Center Configuration Manager consoles.

The Application Catalog, Software Center, and the Company Portal

The **Application Catalog** is a website where users can browse for and request software for their Windows-based PCs. To use the Application Catalog, you must install the Application Catalog web service point and the Application Catalog website point for the site.

Software Center is an application that is installed when the Configuration Manager client is installed on Windows-based computers. Users run this application to request software and manage the software that Configuration Manager deploys to them. Software Center lets users do the following:

- Browse for and install software from the Application Catalog.
- View their software request history.
- Configure when Configuration Manager can install software on their devices.
- Configure access settings for remote control, if an administrative user enabled remote control.

The Company Portal is an app or website that provides similar functions to the Application Catalog, but for mobile devices that are enrolled by Microsoft Intune.

For more information, see Get started with application management in System Center Configuration Manager.

Configuration Manager properties (on Windows PCs)

When the Configuration Manager client is installed on Windows computers, Configuration Manager is installed in Control Panel. Typically, you don't have to configure this application because the client configuration is performed in the Configuration Manager console. This application helps administrative users and the help desk troubleshoot problems with individual clients.

For more information about client deployment, see Client installation methods in System Center Configuration Manager.

Example scenarios for Configuration Manager

The following example scenarios demonstrate how a company named Trey Research uses System Center Configuration Manager to empower users to:

- Be more productive.
- Unify their compliance management for devices for a more streamlined administration experience.
- Simplify device management to reduce IT operating costs.

Example scenario: Empower users by ensuring access to applications from any device

Trey Research wants to ensure that employees have access to the applications that they need, as efficiently as possible. The admin maps these company requirements to the following scenarios:

REQUIREMENT	CURRENT CLIENT MANAGEMENT STATE	FUTURE CLIENT MANAGEMENT STATE
New employees can work efficiently from day one.	When employees join the company, they have to wait for applications to be installed after they first sign in.	When employees join the company, they sign in and their applications are installed and ready to be used.
Employees can quickly and easily request additional software that they need.	When employees need additional applications, they file a ticket with the help desk. Then they typically wait two days for the ticket to be processed and for the applications to be installed.	When employees need additional applications, they can request them from a website. They are installed immediately if there are no licensing restrictions. If there are licensing restrictions, users must first ask for approval before they can install the application. The website shows users only the applications that they're allowed to install.
Employees can use their mobile devices at work if the devices comply with security policies that are monitored and enforced. These policies include enforcing a strong password, locking a device after period of inactivity, and remotely wiping lost or stolen devices.	Employees connect their mobile devices to Exchange Server for email service. But, there is limited reporting to confirm that they are in compliance with the security policies in the default Exchange ActiveSync mailbox policies. The personal use of mobile devices is at risk of being prohibited unless IT can confirm adherence to policy.	The IT organization can report mobile device security compliance with the required settings. This confirmation lets users continue to use their mobile device at work. Users can remotely wipe their mobile device if it's lost or stolen, and the help desk can wipe any user's mobile device that is reported as lost or stolen. Provide mobile device enrollment in a PKI environment for additional security and control.
Employees can be productive even if they're not at their desk.	When employees aren't at their desk and don't have portable computers, they can't access their applications by using the kiosk computers that are available throughout the company.	Employees can use kiosk computers to access their applications and data.

REQUIREMENT	CURRENT CLIENT MANAGEMENT STATE	FUTURE CLIENT MANAGEMENT STATE
Usually, business continuity takes precedence over installing required applications and software updates.	Applications and software updates that are required install during the day and frequently disrupt users from working because their computers slow down or restart during the installation.	Users can configure their working hours to prevent required software from installing while they're using their computer.

To meet the requirements, admins use these Configuration Manager management capabilities and configuration options:

- Application management
- Mobile device management

Admins implement these by using the configuration steps in the following table:

CONFIGURATION STEPS	OUTCOME
The admin makes sure that new users have user accounts in Active Directory and creates a new query-based collection in Configuration Manager for these users. They then defines user device affinity for these users by creating a file that maps the user accounts to the primary computers that they will use and imports this file into Configuration Manager. The applications that new users must have are already created in Configuration Manager. The admin then deploys the applications that have the purpose of Required to the collection that contains the new users.	Because of the user device affinity information, the applications are installed on each user's primary computer or computers before the user signs in. The applications are ready to use as soon as the user successfully signs in.
The admin installs and configures the Application Catalog site system roles so that users can browse for applications to install. They create application deployments that have the purpose of Available, and then deploys these applications to the collection that contains the new users. For the applications that have a restricted number of licenses, the admin configures these applications to require approval.	Users can now use the Application Catalog to browse the applications that they're allowed to install. Users can then either install the applications immediately, or request approval and return to the Application Catalog to install them after the help desk has approved their request.

CONFIGURATION STEPS	OUTCOME
The admin creates an Exchange Server connector in Configuration Manager to manage the mobile devices that connect to the company's on-premises Exchange Server. They configure this connector with security settings that include the requirement to set a strong password and lock the mobile device after a period of inactivity. For additional management for devices that run Windows Phone 8, Windows RT, and iOS, the admin obtains a Microsoft Intune subscription. Then the admin installs the service connection point site system role. This mobile device management solution gives the company greater management support for these devices. This includes making applications available for users to install on these devices and extensive settings management. In addition, mobile device connections are secured by using PKI certificates that are automatically created and deployed by Intune. After configuring the service connection point and subscription for use with Configuration Manager, the admin sends an email message to the users who own these mobile devices for them to click a link to start the enrollment process. For the mobile devices to be enrolled by Microsoft Intune, the admin uses compliance settings to configure security settings for these mobile devices. These settings include the requirement to set a strong password and lock the mobile device after a period of inactivity.	With these two mobile device management solutions, the IT organization can now provide reporting information about the mobile devices that are being used on the company network and their compliance with the configured security settings. Users are shown how to remotely wipe their mobile device by using the Application Catalog or the Company Portal if their mobile device is lost or stolen. The help desk is also instructed how to remotely wipe a mobile device for users by using the Configuration Manager console. In addition, for the mobile devices that are enrolled by Microsoft Intune, the admin can now deploy mobile applications for users to install, collect more inventory data from these devices, and have better management control over these devices by being able to access more settings.
Trey Research has several kiosk computers that are used by employees who visit the office. The employees want their applications to be available to them wherever they sign in. However, the admin doesn't want to locally install all the applications on each computer. To achieve this, the admin creates the required applications that have two deployment types: **The first:** A full, local installation of the application that has a requirement that it can only be installed on a user's primary device. **The second:** A virtual version of the application that has the requirement that it must not be installed on the user's primary device.	When visiting employees sign in to a kiosk computer, they see the applications that they require displayed as icons on the kiosk computer's desktop. When they run the application, it's streamed as a virtual application. This way, they can be as productive as if they're sitting at their desktop.
The admin lets users know that they can configure their business hours in Software Center, and can select options to prevent software deployment activities during this time period and when the computer is in presentation mode.	Because users can control when Configuration Manager deploys software to their computers, users remain more productive during their work day.

These configuration steps and outcomes let Trey Research successfully empower their employees by ensuring access to applications from any device.

Example scenario: Unify compliance management for devices

Trey Research wants a unified client management solution that ensures that their computers run antivirus software that is automatically kept up-to-date. That is:

- Windows Firewall is enabled.

- Critical software updates are installed.
- Specific registry keys are set.
- Managed mobile devices cannot install or run unsigned applications.

The company also wants to extend this protection to the Internet for laptops that move from the intranet to the Internet.

The admin maps these company requirements to the following scenarios:

REQUIREMENT	CURRENT CLIENT MANAGEMENT STATE	FUTURE CLIENT MANAGEMENT STATE
All computers run antimalware software that has up-to-date definition files and enables Windows Firewall.	Different computers run different antimalware solutions that aren't always kept up-to-date. Although Windows Firewall is enabled by default, users sometimes disable it. Users are asked to contact the help desk if malware is detected on their computer.	All computers run the same antimalware solution that automatically downloads the latest definition update files and automatically re-enables Windows Firewall if users disable it. The help desk is automatically notified by email if malware is detected.
All computers install critical software updates within the first month of release.	Although software updates are installed on computers, many computers don't automatically install critical software updates until two or three months after they're released. This leaves them vulnerable to attack during this time period. For the computers that don't install the critical software updates, the help desk first sends out email messages asking users to install the updates. For computers that remain noncompliant, engineers remotely connect to these computers and manually install the missing software updates.	The current compliance rate within the specified month is improved to over 95% without sending email messages or asking the help desk to manually install them.
Security settings for specific applications are regularly checked and remediated if it's necessary.	Computers run complex startup scripts that rely on computer group membership to reset registry values for specific applications. Because these scripts only run at startup and some computers are left on for days, the help desk can't check for configuration drift on a timely basis.	Registry values are checked and automatically remediated without relying on computer group membership or restarting the computer.
Mobile devices can't install or run unsafe applications.	Users are asked not to download and run potentially unsafe applications from the Internet. But there are no controls in place to monitor or enforce this.	Mobile devices that are managed with Microsoft Intune or Configuration Manager automatically prevent unsigned applications from installing or running.
Laptops that move from the intranet to the Internet must be kept secure.	For users who travel, they frequently can't connect over the VPN connection daily. These laptops become out of compliance with security requirements.	An Internet connection is all that is required for laptops to be kept in compliance with security requirements. Users don't have to sign in or use the VPN connection.

To meet the requirements, the admin uses these Configuration Manager management capabilities and

configuration options:

- Endpoint Protection
- Software updates
- Compliance settings
- Mobile device management
- Internet-based client management

He implements these by using the configuration steps in the following table:

CONFIGURATION STEPS	OUTCOME
The admin configures Endpoint Protection. They enable the client setting to uninstall other antimalware solutions and enables Windows Firewall. The admin configures automatic deployment rules so that computers check for and install the latest definition updates regularly.	The single antimalware solution helps protect all computers by using minimal administrative overhead. Because the help desk is automatically notified by an email message if antimalware is detected, problems can be resolved quickly. This helps prevent attacks on other computers.
To help increase compliance rates, the admin uses automatic deployment rules, defines maintenance windows for servers, and investigates the advantages and disadvantages of using Wake-on-LAN for computers that hibernate.	Compliance for critical software updates increases and reduces the requirement for users or the help desk to install software updates manually.
The admin uses compliance settings to check for the presence of the specified applications. When the applications are detected, configuration items then check the registry values and automatically remediate them if they're out of compliance.	By using configuration items and configuration baselines that are deployed to all computers and check for compliance every day, you no longer require separate scripts that rely on computer membership and computer restarts.
The admin uses compliance settings for enrolled mobile devices and configures the Exchange Server connector so that unsigned applications are prohibited from installing and running on mobile devices.	Because unsigned applications are prohibited, mobile devices are automatically protected from potentially harmful applications.
The admin makes sure that site system servers and computers have the PKI certificates that Configuration Manager requires for HTTPS connections. Then they install additional site system roles in the perimeter network that accept client connections from the Internet.	Computers that move from the intranet to the Internet automatically continue to be managed by Configuration Manager when they have an Internet connection. Those computers don't rely on users signing in to their computer or connecting to the VPN connection. These computers continue to be managed for antimalware and Windows Firewall, software updates, and configuration items. As a result, compliance levels automatically increase.

These configuration steps and outcomes result in Trey Research successfully unifying their compliance management for devices.

Example scenario: Simplify client management for devices

Trey Research wants all new computers to automatically install their company's base computer image that runs Windows 7. After the operating system image is installed on these computers, they must be managed and monitored for additional software that users install. Computers that store highly confidential information require more restrictive management policies than the other computers. For example, help desk engineers must not connect to them remotely, BitLocker PIN entry must be used for restarts, and only local administrators can install software.

The admin maps these company requirements to the following scenarios:

REQUIREMENT	CURRENT CLIENT MANAGEMENT STATE	FUTURE CLIENT MANAGEMENT STATE
New computers are installed with Windows 7.	The help desk installs and configures Windows 7 for users, and then sends the computer to the respective location.	New computers go straight to the final destination, are plugged into the network, and automatically install and configure Windows 7.
Computers must be managed and monitored. This includes collecting hardware and software inventory data to help determine licensing requirements.	The Configuration Manager client is deployed by using automatic client push installation. The help desk investigates installation failures and clients that don't send inventory data when it's expected. Failures are frequent because of installation dependencies that aren't met and WMI corruption on the client.	Client installation and inventory data that is collected from computers is more reliable and requires less intervention from the help desk. Reports show software usage for license information.
Some computers must have more rigorous management policies.	Because of the more rigorous management policies, these computers are currently not managed by Configuration Manager.	These computers are managed by using Configuration Manager to accommodate exceptions without additional administrative overhead.

To meet the requirements, the admin uses these Configuration Manager management capabilities and configuration options:

- Operating system deployment
- Client deployment and client status
- Compliance settings
- Client settings
- Inventory methods and Asset Intelligence
- Role-based administration

He implements these by using the configuration steps in the following table:

CONFIGURATION STEPS	OUTCOME
The admin captures an operating system image from a computer that has Windows 7 installed and is configured to the company specifications. They then deploys the operating system to the new computers by using unknown computer support and PXE. The admin also installs the Configuration Manager client as part of the operating system deployment.	New computers are up and running more quickly without intervention from the help desk.

CONFIGURATION STEPS	OUTCOME
The admin configures automatic site-wide client push installation to install the Configuration Manager client on any computers that are discovered. This ensures that any computers that were not imaged with the client still install the client so that the computer is managed by Configuration Manager. The admin configures client status to automatically remediate any client issues that are discovered. They also configure client settings that enable the collection of inventory data that is required and configures Asset Intelligence.	Installing the client together with the operating system is quicker and more reliable than waiting for Configuration Manager to discover the computer and then trying to install the client source files on the computer. However, by leaving the automatic client push option enabled, you provide a backup method for a computer that already has the operating system installed to install the client when the computer connects to the network. Client settings ensure that clients send their inventory information to the site regularly. This, in addition to the client status tests, helps to keep the client running with minimal intervention from the help desk. For example, WMI corruptions are detected and automatically remediated. The Asset Intelligence reports help monitor software usage and licenses.
The admin creates a collection for the computers that must have more rigorous policy settings. Then they create a custom client device setting for this collection that disables remote control, enables BitLocker PIN entry, and lets only local administrators install software. The admin configures role-based administration so that help desk engineers don't see this collection of computers. This helps ensure that these computers aren't accidentally managed as standard computers.	These computers are now managed by Configuration Manager, but with specific settings that don't require a new site. The collection for these computers isn't visible to the help desk engineers. This helps reduce the possibility of the computers being accidentally sent deployments and scripts for standard computers.

These configuration steps and outcomes result in Trey Research successfully simplifying client management for devices.

Next steps

Before you install Configuration Manager, you can become familiar with some basic concepts and terms that are specific to Configuration Manager.

- If you're familiar with System Center 2012 Configuration Manager, see What's changed in System Center Configuration Manager from System Center 2012 Configuration Manager to understand the new capabilities.
- For a high-level technical overview of System Center Configuration Manager, see Fundamentals of System Center Configuration Manager.

When you're familiar with the basic concepts, use the System Center Configuration Manager documentation to help you successfully deploy and use Configuration Manager.

Introduction to System Center Configuration Manager

5/23/2019 • 19 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

A product in the Microsoft System Center suite of management solutions, System Center Configuration Manager can help you manage devices and users both on-premises and in the cloud.

You can use Configuration Manager to help you:

- Increase IT productivity and efficiency by reducing manual tasks and letting you focus on high-value projects.
- Maximize hardware and software investments.
- Empower user productivity by providing the right software at the right time.

Configuration Manager helps you deliver more effective IT services by enabling:

- Secure and scalable software deployment.
- Compliance settings management.
- Comprehensive asset management of servers, desktops, laptops, and mobile devices.

Configuration Manager extends and works alongside your existing Microsoft technologies and solutions.

For example, Configuration Manager integrates with:

- Microsoft Intune to manage a wide variety of mobile device platforms.
- Windows Server Update Services (WSUS) to manage software updates.
- Certificate Services.
- Exchange Server and Exchange Online.
- Windows Group Policy.
- DNS.
- Windows Automated Deployment Kit (Windows ADK) and the User State Migration Tool (USMT).
- Windows Deployment Services (WDS).
- Remote Desktop and Remote Assistance.

Configuration Manager also uses:

- Active Directory Domain Services for security, service location, configuration, and to discover the users and devices that you want to manage.
- Microsoft SQL Server as a distributed change management database—and integrates with SQL Server Reporting Services (SSRS) to produce reports to monitor and track management activities.
- Site system roles that extend management functionality and use the web services of Internet Information Services (IIS).
- Background Intelligent Transfer Service (BITS) and BranchCache to help manage the available network bandwidth.

To be successful with Configuration Manager, you must first thoroughly plan and test the management features before you use Configuration Manager in a production environment. As a powerful management application, Configuration Manager has the potential to affect every computer in your organization. When you deploy and

manage Configuration Manager with careful planning and consideration of your business requirements, Configuration Manager can reduce your administrative overhead and total cost of ownership.

Use the following topics and additional sections in this topic to learn more about Configuration Manager.

Related topics in this documentation library:

- Features and capabilities of System Center Configuration Manager
- Choose a device management solution for System Center Configuration Manager
- What's changed in System Center Configuration Manager from System Center 2012 Configuration Manager
- Fundamentals of System Center Configuration Manager
- Evaluate System Center Configuration Manager by building your own lab environment
- Find help for using System Center Configuration Manager
- Removed and deprecated items for System Center Configuration Manager

The Configuration Manager console

After you install Configuration Manager, use the Configuration Manager console to configure sites and clients, and to run and monitor management tasks. This console is the main point of administration and lets you manage multiple sites.

You can use the console to run secondary consoles that provide support for specific client management tasks, like:

- **Resource Explorer**, to view hardware and software inventory information.
- **Remote control**, to remotely connect to a client computer to perform troubleshooting tasks.

You can install the Configuration Manager console on additional computers, and restrict access and limit what administrative users can see in the console by using Configuration Manager role-based administration.

For more information, see Install System Center Configuration Manager consoles.

The Application Catalog, Software Center, and the Company Portal

The **Application Catalog** is a website where users can browse for and request software for their Windows-based PCs. To use the Application Catalog, you must install the Application Catalog web service point and the Application Catalog website point for the site.

Software Center is an application that is installed when the Configuration Manager client is installed on Windows-based computers. Users run this application to request software and manage the software that Configuration Manager deploys to them. Software Center lets users do the following:

- Browse for and install software from the Application Catalog.
- View their software request history.
- Configure when Configuration Manager can install software on their devices.
- Configure access settings for remote control, if an administrative user enabled remote control.

The Company Portal is an app or website that provides similar functions to the Application Catalog, but for mobile devices that are enrolled by Microsoft Intune.

For more information, see Get started with application management in System Center Configuration Manager.

Configuration Manager properties (on Windows PCs)

When the Configuration Manager client is installed on Windows computers, Configuration Manager is installed in Control Panel. Typically, you don't have to configure this application because the client configuration is performed in the Configuration Manager console. This application helps administrative users and the help desk troubleshoot problems with individual clients.

For more information about client deployment, see Client installation methods in System Center Configuration Manager.

Example scenarios for Configuration Manager

The following example scenarios demonstrate how a company named Trey Research uses System Center Configuration Manager to empower users to:

- Be more productive.
- Unify their compliance management for devices for a more streamlined administration experience.
- Simplify device management to reduce IT operating costs.

Example scenario: Empower users by ensuring access to applications from any device

Trey Research wants to ensure that employees have access to the applications that they need, as efficiently as possible. The admin maps these company requirements to the following scenarios:

REQUIREMENT	CURRENT CLIENT MANAGEMENT STATE	FUTURE CLIENT MANAGEMENT STATE
New employees can work efficiently from day one.	When employees join the company, they have to wait for applications to be installed after they first sign in.	When employees join the company, they sign in and their applications are installed and ready to be used.
Employees can quickly and easily request additional software that they need.	When employees need additional applications, they file a ticket with the help desk. Then they typically wait two days for the ticket to be processed and for the applications to be installed.	When employees need additional applications, they can request them from a website. They are installed immediately if there are no licensing restrictions. If there are licensing restrictions, users must first ask for approval before they can install the application. The website shows users only the applications that they're allowed to install.
Employees can use their mobile devices at work if the devices comply with security policies that are monitored and enforced. These policies include enforcing a strong password, locking a device after period of inactivity, and remotely wiping lost or stolen devices.	Employees connect their mobile devices to Exchange Server for email service. But, there is limited reporting to confirm that they are in compliance with the security policies in the default Exchange ActiveSync mailbox policies. The personal use of mobile devices is at risk of being prohibited unless IT can confirm adherence to policy.	The IT organization can report mobile device security compliance with the required settings. This confirmation lets users continue to use their mobile device at work. Users can remotely wipe their mobile device if it's lost or stolen, and the help desk can wipe any user's mobile device that is reported as lost or stolen. Provide mobile device enrollment in a PKI environment for additional security and control.
Employees can be productive even if they're not at their desk.	When employees aren't at their desk and don't have portable computers, they can't access their applications by using the kiosk computers that are available throughout the company.	Employees can use kiosk computers to access their applications and data.

REQUIREMENT	CURRENT CLIENT MANAGEMENT STATE	FUTURE CLIENT MANAGEMENT STATE
Usually, business continuity takes precedence over installing required applications and software updates.	Applications and software updates that are required install during the day and frequently disrupt users from working because their computers slow down or restart during the installation.	Users can configure their working hours to prevent required software from installing while they're using their computer.

To meet the requirements, admins use these Configuration Manager management capabilities and configuration options:

- Application management
- Mobile device management

Admins implement these by using the configuration steps in the following table:

CONFIGURATION STEPS	OUTCOME
The admin makes sure that new users have user accounts in Active Directory and creates a new query-based collection in Configuration Manager for these users. They then defines user device affinity for these users by creating a file that maps the user accounts to the primary computers that they will use and imports this file into Configuration Manager. The applications that new users must have are already created in Configuration Manager. The admin then deploys the applications that have the purpose of Required to the collection that contains the new users.	Because of the user device affinity information, the applications are installed on each user's primary computer or computers before the user signs in. The applications are ready to use as soon as the user successfully signs in.
The admin installs and configures the Application Catalog site system roles so that users can browse for applications to install. They create application deployments that have the purpose of Available, and then deploys these applications to the collection that contains the new users. For the applications that have a restricted number of licenses, the admin configures these applications to require approval.	Users can now use the Application Catalog to browse the applications that they're allowed to install. Users can then either install the applications immediately, or request approval and return to the Application Catalog to install them after the help desk has approved their request.

CONFIGURATION STEPS	OUTCOME
The admin creates an Exchange Server connector in Configuration Manager to manage the mobile devices that connect to the company's on-premises Exchange Server. They configure this connector with security settings that include the requirement to set a strong password and lock the mobile device after a period of inactivity. For additional management for devices that run Windows Phone 8, Windows RT, and iOS, the admin obtains a Microsoft Intune subscription. Then the admin installs the service connection point site system role. This mobile device management solution gives the company greater management support for these devices. This includes making applications available for users to install on these devices and extensive settings management. In addition, mobile device connections are secured by using PKI certificates that are automatically created and deployed by Intune. After configuring the service connection point and subscription for use with Configuration Manager, the admin sends an email message to the users who own these mobile devices for them to click a link to start the enrollment process. For the mobile devices to be enrolled by Microsoft Intune, the admin uses compliance settings to configure security settings for these mobile devices. These settings include the requirement to set a strong password and lock the mobile device after a period of inactivity.	With these two mobile device management solutions, the IT organization can now provide reporting information about the mobile devices that are being used on the company network and their compliance with the configured security settings. Users are shown how to remotely wipe their mobile device by using the Application Catalog or the Company Portal if their mobile device is lost or stolen. The help desk is also instructed how to remotely wipe a mobile device for users by using the Configuration Manager console. In addition, for the mobile devices that are enrolled by Microsoft Intune, the admin can now deploy mobile applications for users to install, collect more inventory data from these devices, and have better management control over these devices by being able to access more settings.
Trey Research has several kiosk computers that are used by employees who visit the office. The employees want their applications to be available to them wherever they sign in. However, the admin doesn't want to locally install all the applications on each computer. To achieve this, the admin creates the required applications that have two deployment types: **The first:** A full, local installation of the application that has a requirement that it can only be installed on a user's primary device. **The second:** A virtual version of the application that has the requirement that it must not be installed on the user's primary device.	When visiting employees sign in to a kiosk computer, they see the applications that they require displayed as icons on the kiosk computer's desktop. When they run the application, it's streamed as a virtual application. This way, they can be as productive as if they're sitting at their desktop.
The admin lets users know that they can configure their business hours in Software Center, and can select options to prevent software deployment activities during this time period and when the computer is in presentation mode.	Because users can control when Configuration Manager deploys software to their computers, users remain more productive during their work day.

These configuration steps and outcomes let Trey Research successfully empower their employees by ensuring access to applications from any device.

Example scenario: Unify compliance management for devices

Trey Research wants a unified client management solution that ensures that their computers run antivirus software that is automatically kept up-to-date. That is:

- Windows Firewall is enabled.

- Critical software updates are installed.
- Specific registry keys are set.
- Managed mobile devices cannot install or run unsigned applications.

The company also wants to extend this protection to the Internet for laptops that move from the intranet to the Internet.

The admin maps these company requirements to the following scenarios:

REQUIREMENT	CURRENT CLIENT MANAGEMENT STATE	FUTURE CLIENT MANAGEMENT STATE
All computers run antimalware software that has up-to-date definition files and enables Windows Firewall.	Different computers run different antimalware solutions that aren't always kept up-to-date. Although Windows Firewall is enabled by default, users sometimes disable it. Users are asked to contact the help desk if malware is detected on their computer.	All computers run the same antimalware solution that automatically downloads the latest definition update files and automatically re-enables Windows Firewall if users disable it. The help desk is automatically notified by email if malware is detected.
All computers install critical software updates within the first month of release.	Although software updates are installed on computers, many computers don't automatically install critical software updates until two or three months after they're released. This leaves them vulnerable to attack during this time period. For the computers that don't install the critical software updates, the help desk first sends out email messages asking users to install the updates. For computers that remain noncompliant, engineers remotely connect to these computers and manually install the missing software updates.	The current compliance rate within the specified month is improved to over 95% without sending email messages or asking the help desk to manually install them.
Security settings for specific applications are regularly checked and remediated if it's necessary.	Computers run complex startup scripts that rely on computer group membership to reset registry values for specific applications. Because these scripts only run at startup and some computers are left on for days, the help desk can't check for configuration drift on a timely basis.	Registry values are checked and automatically remediated without relying on computer group membership or restarting the computer.
Mobile devices can't install or run unsafe applications.	Users are asked not to download and run potentially unsafe applications from the Internet. But there are no controls in place to monitor or enforce this.	Mobile devices that are managed with Microsoft Intune or Configuration Manager automatically prevent unsigned applications from installing or running.
Laptops that move from the intranet to the Internet must be kept secure.	For users who travel, they frequently can't connect over the VPN connection daily. These laptops become out of compliance with security requirements.	An Internet connection is all that is required for laptops to be kept in compliance with security requirements. Users don't have to sign in or use the VPN connection.

To meet the requirements, the admin uses these Configuration Manager management capabilities and

configuration options:

- Endpoint Protection
- Software updates
- Compliance settings
- Mobile device management
- Internet-based client management

He implements these by using the configuration steps in the following table:

CONFIGURATION STEPS	OUTCOME
The admin configures Endpoint Protection. They enable the client setting to uninstall other antimalware solutions and enables Windows Firewall. The admin configures automatic deployment rules so that computers check for and install the latest definition updates regularly.	The single antimalware solution helps protect all computers by using minimal administrative overhead. Because the help desk is automatically notified by an email message if antimalware is detected, problems can be resolved quickly. This helps prevent attacks on other computers.
To help increase compliance rates, the admin uses automatic deployment rules, defines maintenance windows for servers, and investigates the advantages and disadvantages of using Wake-on-LAN for computers that hibernate.	Compliance for critical software updates increases and reduces the requirement for users or the help desk to install software updates manually.
The admin uses compliance settings to check for the presence of the specified applications. When the applications are detected, configuration items then check the registry values and automatically remediate them if they're out of compliance.	By using configuration items and configuration baselines that are deployed to all computers and check for compliance every day, you no longer require separate scripts that rely on computer membership and computer restarts.
The admin uses compliance settings for enrolled mobile devices and configures the Exchange Server connector so that unsigned applications are prohibited from installing and running on mobile devices.	Because unsigned applications are prohibited, mobile devices are automatically protected from potentially harmful applications.
The admin makes sure that site system servers and computers have the PKI certificates that Configuration Manager requires for HTTPS connections. Then they install additional site system roles in the perimeter network that accept client connections from the Internet.	Computers that move from the intranet to the Internet automatically continue to be managed by Configuration Manager when they have an Internet connection. Those computers don't rely on users signing in to their computer or connecting to the VPN connection. These computers continue to be managed for antimalware and Windows Firewall, software updates, and configuration items. As a result, compliance levels automatically increase.

These configuration steps and outcomes result in Trey Research successfully unifying their compliance management for devices.

Example scenario: Simplify client management for devices

Trey Research wants all new computers to automatically install their company's base computer image that runs Windows 7. After the operating system image is installed on these computers, they must be managed and monitored for additional software that users install. Computers that store highly confidential information require more restrictive management policies than the other computers. For example, help desk engineers must not connect to them remotely, BitLocker PIN entry must be used for restarts, and only local administrators can install software.

The admin maps these company requirements to the following scenarios:

REQUIREMENT	CURRENT CLIENT MANAGEMENT STATE	FUTURE CLIENT MANAGEMENT STATE
New computers are installed with Windows 7.	The help desk installs and configures Windows 7 for users, and then sends the computer to the respective location.	New computers go straight to the final destination, are plugged into the network, and automatically install and configure Windows 7.
Computers must be managed and monitored. This includes collecting hardware and software inventory data to help determine licensing requirements.	The Configuration Manager client is deployed by using automatic client push installation. The help desk investigates installation failures and clients that don't send inventory data when it's expected. Failures are frequent because of installation dependencies that aren't met and WMI corruption on the client.	Client installation and inventory data that is collected from computers is more reliable and requires less intervention from the help desk. Reports show software usage for license information.
Some computers must have more rigorous management policies.	Because of the more rigorous management policies, these computers are currently not managed by Configuration Manager.	These computers are managed by using Configuration Manager to accommodate exceptions without additional administrative overhead.

To meet the requirements, the admin uses these Configuration Manager management capabilities and configuration options:

- Operating system deployment
- Client deployment and client status
- Compliance settings
- Client settings
- Inventory methods and Asset Intelligence
- Role-based administration

He implements these by using the configuration steps in the following table:

CONFIGURATION STEPS	OUTCOME
The admin captures an operating system image from a computer that has Windows 7 installed and is configured to the company specifications. They then deploys the operating system to the new computers by using unknown computer support and PXE. The admin also installs the Configuration Manager client as part of the operating system deployment.	New computers are up and running more quickly without intervention from the help desk.

CONFIGURATION STEPS	OUTCOME
The admin configures automatic site-wide client push installation to install the Configuration Manager client on any computers that are discovered. This ensures that any computers that were not imaged with the client still install the client so that the computer is managed by Configuration Manager. The admin configures client status to automatically remediate any client issues that are discovered. They also configure client settings that enable the collection of inventory data that is required and configures Asset Intelligence.	Installing the client together with the operating system is quicker and more reliable than waiting for Configuration Manager to discover the computer and then trying to install the client source files on the computer. However, by leaving the automatic client push option enabled, you provide a backup method for a computer that already has the operating system installed to install the client when the computer connects to the network. Client settings ensure that clients send their inventory information to the site regularly. This, in addition to the client status tests, helps to keep the client running with minimal intervention from the help desk. For example, WMI corruptions are detected and automatically remediated. The Asset Intelligence reports help monitor software usage and licenses.
The admin creates a collection for the computers that must have more rigorous policy settings. Then they create a custom client device setting for this collection that disables remote control, enables BitLocker PIN entry, and lets only local administrators install software. The admin configures role-based administration so that help desk engineers don't see this collection of computers. This helps ensure that these computers aren't accidentally managed as standard computers.	These computers are now managed by Configuration Manager, but with specific settings that don't require a new site. The collection for these computers isn't visible to the help desk engineers. This helps reduce the possibility of the computers being accidentally sent deployments and scripts for standard computers.

These configuration steps and outcomes result in Trey Research successfully simplifying client management for devices.

Next steps

Before you install Configuration Manager, you can become familiar with some basic concepts and terms that are specific to Configuration Manager.

- If you're familiar with System Center 2012 Configuration Manager, see What's changed in System Center Configuration Manager from System Center 2012 Configuration Manager to understand the new capabilities.
- For a high-level technical overview of System Center Configuration Manager, see Fundamentals of System Center Configuration Manager.

When you're familiar with the basic concepts, use the System Center Configuration Manager documentation to help you successfully deploy and use Configuration Manager.

Find help for using Configuration Manager

7/19/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article provides the following sections with multiple resources to find help for using Configuration Manager:

- Product documentation
- Sharing product feedback
- Follow the Configuration Manager team blog
- Support options and community resources

For help with product accessibility, see Accessibility features.

Product documentation

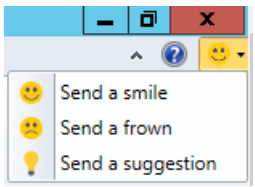
To access the most current product documentation, start at the library index.

For tips on searching, providing feedback, and more information about using the product documentation, see How to use the docs.

Product feedback starting with version 1806

Starting in Configuration Manager version 1806, you can send product feedback directly from the console. If you need to attach logs, use Feedback Hub. You can do the following things:

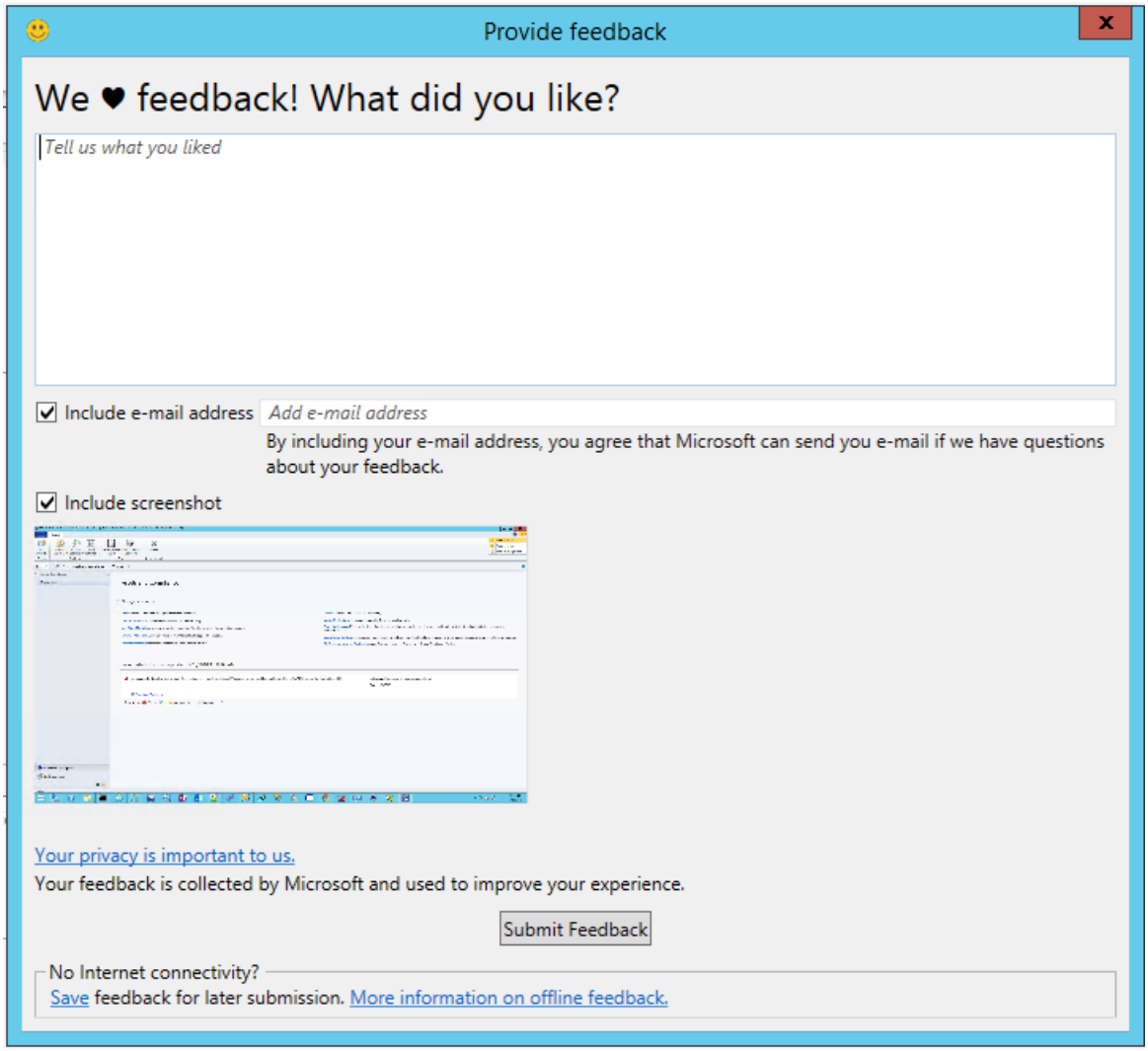
- **Send a smile**: Send feedback on what you liked.
- **Send a frown**: Send feedback on what you didn't like.
- **Send a suggestion**: Takes you to the UserVoice website to share your idea.



Send a smile

To send feedback on something that you liked follow the instructions below:

1. In the upper right corner of the console, click on the smiley face.
2. In the drop-down menu, select **Send a smile**.
3. Use the text box to explain what you liked.
4. Choose if you would like to share your e-mail address and a screenshot.
5. Click **Submit Feedback**
   - If you don't have internet connectivity, click on **Save** at the bottom. Follow the instructions in the Send feedback that you saved for later submission section to send it to Microsoft.



Send a frown

To send feedback on something that you didn't like, follow the instructions below:

1. In the upper right corner of the console, click on the smiley face.
2. In the drop-down menu, select **Send a frown**.
3. Use the text box to explain what you didn't like.
4. Choose if you would like to share your e-mail address and a screenshot.
5. Click **Submit Feedback**
   - If you don't have internet connectivity, click on **Save** at the bottom. Follow the instructions in the Send feedback that you saved for later submission section to send it to Microsoft.

Send a suggestion

When you **Send a suggestion**, you're directed to UserVoice, a third-party website, to share your idea. The Configuration Manager product team uses the following UserVoice status values:

- **Noted** - We understand the request and it makes sense. We've added it to our backlog.
- **Planned** - We've started coding for this feature and expect it to show up in a tech preview build within the next few months.
- **Started** - The feature is now in a tech preview. Go check it out, and give us feedback. Let us know if the feature is on the right track or not. Put additional feedback in the comments section of the original request for others to see and comment on. We'll read that and use the feedback to try to improve the feature.
- **Completed** - The first version of the feature is in a production build. This status doesn't mean we're 100% done with the feature, and will no longer improve it. But it does mean that v1 of the features is in a production build, and you can start using it for real. We're marking it completed because:
  - We want you to know the feature is production ready.

- We want to give back your UserVoice votes so you can use them on other items.
- You can file new Design Change Requests to this feature to help us know the next most important improvement for this feature.

Information sent with feedback

When you **Send a smile** or **Send a frown**, the following information is sent with the feedback:

- OS build information
- Configuration Manager hierarchy ID
- Product build information
- Language information
- Device identifier
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient:MachineId

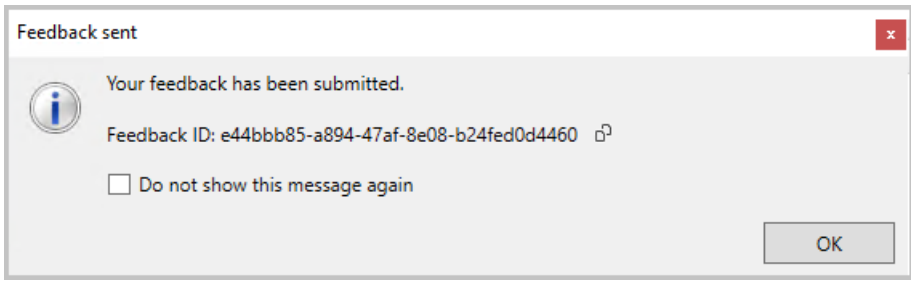
Send feedback that you saved for later submission

1. Click on **Save** at the bottom of the **Provide feedback** window.
2. Save the .zip file. If the local machine doesn't have internet access, copy the file to an internet connected machine.
3. If needed, copy UploadOfflineFeedback folder located at `cd.latest\SMSSETUP\Tools\UploadOfflineFeedback\`
   - For more information about the cd.latest folder, see The CD.Latest folder
4. On an internet connected machine, open a command prompt.
5. Run the following command: `UploadOfflineFeedback.exe -f c:\folder\location_of.zip`
   - Optionally, you can specify the following parameters:
     - `-t, --timeout` Timeout in seconds for sending the data. 0 is unlimited. Default is 30.
     - `-s --silent` No logging to console (Cannot combine with --verbose)
     - `-v, --verbose` Output verbose logging to console (Cannot combine with --silent)
     - `--help` Displays the help screen

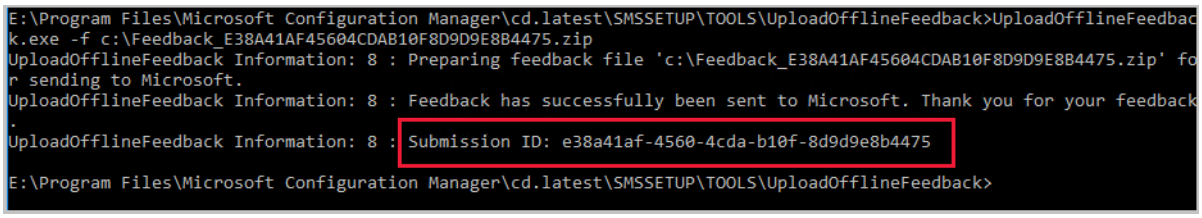
Confirmation of console feedback

Starting in version 1902, when you send feedback through the Configuration Manager console or UploadOfflineFeedback.exe, it shows a confirmation message. This message includes a **Feedback ID**, which you can give to Microsoft as a tracking identifier.

- To copy the **Feedback ID**, select the copy icon next to the ID, or use the **CTRL** + **C** key shortcut.
  - This ID isn't stored on your computer, so make sure to copy it before closing the window.
- Clicking on **Do not show this message again** will suppress the dialog box and prevent it from appearing in the future.



- The **UploadOfflineFeedback** command tool writes the **FeedbackID** to the console unless -s or --silent is used.



Product feedback for versions 1802 and earlier

Report potential product defects through the Feedback Hub app built-in to Windows 10. When you **Add new feedback**, be sure to select the **Enterprise Management** category, and then choose from one of the following subcategories:

- Configuration Manager Client
- Configuration Manager Console
- Configuration Manager OS Deployment
- Configuration Manager Server

Continue to use the UserVoice page to vote on new feature ideas in Configuration Manager. The Configuration Manager product team uses the following UserVoice status values:

- **Noted** - We understand the request and it makes sense. We've added it to our backlog.
- **Planned** - We've started coding for this feature and expect it to show up in a tech preview build within the next few months.
- **Started** - The feature is now in a tech preview. Go check it out, and give us feedback. Let us know if the feature is on the right track or not. Put additional feedback in the comments section of the original request for others to see and comment on. We'll read that and use the feedback to try to improve the feature.
- **Completed** - The first version of the feature is in a production build. This status doesn't mean we're 100% done with the feature, and will no longer improve it. But it does mean that v1 of the features is in a production build, and you can start using it for real. We're marking it completed because:
  - We want you to know the feature is production ready.
  - We want to give back your UserVoice votes so you can use them on other items.
  - You can file new Design Change Requests to this feature to help us know the next most important improvement for this feature.

Configuration Manager team blog

The Configuration Manager engineering and partner teams use the Enterprise Mobility + Security blog to provide you with technical information and other news about Configuration Manager and related technologies. Our blog posts supplement the product documentation and support information.

Support options and community resources

The following links provide information about support options and community resources:

- Microsoft support
- Configuration Manager Community: System Center Configuration Manager (Current Branch) Survival Guide
- Configuration Manager forums page

How to use the Configuration Manager docs

6/20/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article provides the following sections with multiple resources and tips for using the Configuration Manager documentation library:

- How to search
- Submitting doc bugs, enhancements, questions and new ideas
- How to get notified of changes
- How to contribute to docs

For general help with the product, see Find help.

Search

Use the following search tips to help you find the information that you need:

- When using your preferred search engine to locate content for Configuration Manager, include `SCCM` along with your search keywords.
  - Look for results from docs.microsoft.com for Configuration Manager current branch. Results from technet.microsoft.com or msdn.microsoft.com are for older product versions.
  - To further focus the search results to the current content library, include `site:docs.microsoft.com` to scope the search engine.
- Use search terms that match terminology in the user interface and online documentation. Avoid unofficial terms or abbreviations that you might see in community content. For example, search for "management point" rather than "MP"; "deployment type" rather than "DT"; and "software updates" rather than "SUM."
- To search within an article you are currently viewing, use your browser's **Find** feature. With most modern web browsers, press **Ctrl**+**F** and then enter your search terms.
- Each article on docs.microsoft.com includes the following fields to assist with searching the content:
  - **Search** in the upper right corner. To search all articles enter terms in this field. Articles in the Configuration Manager library automatically include the "ConfigMgr" scope.
  - **Filter by title** above the left table of contents. To search the current table of contents, enter terms in this field. This field only matches terms that appear in the article titles for the current node. For example, Core Infrastructure or Application Management.
- Having problems finding something? File feedback! When filing the issue, provide the search engine you're using, the keywords you tried, and the target article. This feedback helps Microsoft optimize the content for better search.

TIP

Starting in Configuration Manager version 1902, there's a **Documentation** node in the new **Community** workspace. This node includes up-to-date information about Configuration Manager documentation and support articles. For more information, see Using the Configuration Manager console

Feedback

Go to the Feedback section at the bottom by clicking the **Feedback** link in the upper right of any article. This section is integrated with GitHub Issues. For more information about integration with GitHub Issues, see the docs platform blog post.

To share feedback on the Configuration Manager product itself, click **Product feedback**. For more information, see Product feedback.

A GitHub account is a prerequisite for providing documentation feedback. Once you sign in, there is a one-time authorization for MicrosoftDocs. Then when you click **Content feedback**, enter a title and comment, and then **Submit feedback**. This action files a new issue for the target article in the SCCMdocs repository.

This integration also displays any existing open or closed issues for the target article. If any exist, review them before submitting a new issue. If you find a related issue, click the face icon to add a reaction, or you can expand it to add a comment.

Types of feedback

Use GitHub Issues to submit the following types of feedback:

- Doc bug: The content is out of date, unclear, confusing, or broken.
- Doc enhancement: A suggestion to improve the article.
- Doc question: You need help finding existing documentation.
- Doc idea: A suggestion for a new article. Use this method instead of UserVoice for documentation feedback.
- Kudos: Positive feedback about a helpful or informative article!
- Localization: Feedback about content translation.
- Search engine optimization (SEO): Feedback about problems searching for content. Include the search engine, keywords, and target article in the comments.

If issues are raised for non-doc-related topics, such as product feedback, product questions, or support requests, these issues will be closed and the user redirected to the proper feedback channel.

To share feedback on the docs.microsoft.com platform, see Docs feedback. The platform includes all of the wrapper components such as the header, table of contents, and right menu. Also how the articles render in the browser, such as the font, alert boxes, and page anchors.

Notifications

To receive notifications when content changes in the documentation library, use the following steps:

1. Use the docs search to find an article or set of articles. For example:
   - Search for a single article by title: "Log files for troubleshooting - Configuration Manager"
   - Search for any article regarding SQL
2. In the upper right corner, click the **RSS** link.
3. Use this feed in any RSS application to receive notifications when there is a change to any of the search results.

> **TIP**
> You can also **Watch** the SCCMdocs repository on GitHub. This method generates a lot of notifications. It also doesn't include changes from a private repository used by Microsoft.

Contribute

The Configuration Manager documentation library, like most content on docs.microsoft.com, is open-sourced on GitHub. This library accepts and encourages community contributions. For more information on how to get started, see the Contributor Guide. Creating a GitHub account is the only prerequisite.

Basic steps to contribute to SCCMdocs

1. From the target article, click **Edit**. This action opens the source file in GitHub.
2. To edit the source file, click the pencil icon.
3. Make changes in the markdown source. For more information, see How to use Markdown for writing Docs.
4. In the Propose file change section, enter the public commit comment describing *what* you changed. Then click **Propose file change**.
5. Scroll down and verify the changes you made. Click **Create pull request** to open the form. Describe *why* you made this change. Tag the article author and request that they review. Click **Create pull request**.

What to contribute

If you're interested in contributing, but don't know where to start, see the following suggestions:

- Search the list of issues for the community-targeted labels:
  - good-first-issue
  - help-wanted

    These labels are assigned by Microsoft authors to issues that are good candidates for community contribution.
- Review an article for accuracy. Then update the **ms.date** metadata using `mm/dd/yyyy` format. This contribution helps keep the content fresh.
- Add clarifications, examples, or guidance based on your experience. This contribution uses the power of the community to share knowledge.
- Correct translations in a non-English language. This contribution improves the usability of localized content.

> **NOTE**
> Large contributions require signing a Contribution License Agreement (CLA) if you aren't a Microsoft employee. GitHub automatically requires you to sign this agreement when a contribution meets the threshold.

Tips

Follow these general guidelines when contributing to Configuration Manager docs:

- Don't surprise us with large pull requests. Instead, file an issue and start a discussion. Then we can agree on a direction before you invest a large amount of time.
- Read the Microsoft style guide. Know the Top 10 tips for Microsoft style and voice.
- Use the pull request template as the starting point of your work.

- Follow the GitHub Flow workflow.
- Blog and tweet (or whatever) about your contributions, frequently!

(This list was borrowed from the .NET contributing guide.)

Using the Configuration Manager console

8/16/2019 • 13 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

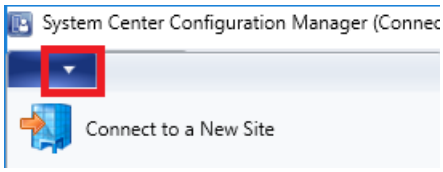
Administrators use the Configuration Manager console to manage the Configuration Manager environment. This article covers the fundamentals of navigating the console.

Connect to a site server

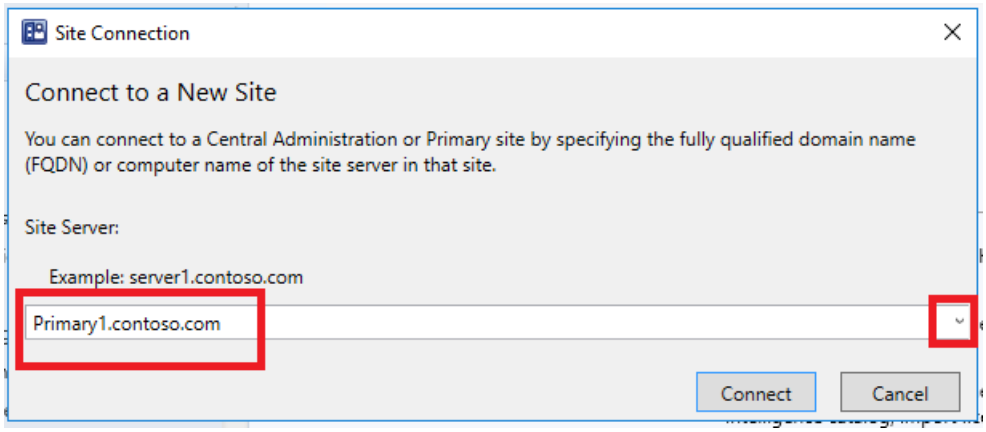
The console connects to your central administration site server or to your primary site servers. You can't connect a Configuration Manager console to a secondary site. You can install the Configuration Manager console. During installation, you specified the fully qualified domain name (FQDN) of the site server to which the console connects.

To connect to a different site server, use the following steps:

1. Select the arrow at the top of the ribbon, and choose **Connect to a New Site**.



2. Type in the FQDN of the site server. If you've previously connected to site server, select the server from the drop-down list.



3. Select **Connect**.

Starting in version 1810, you can specify the minimum authentication level for administrators to access Configuration Manager sites. This feature enforces administrators to sign in to Windows with the required level. For more information, see Plan for the SMS Provider.

Navigation

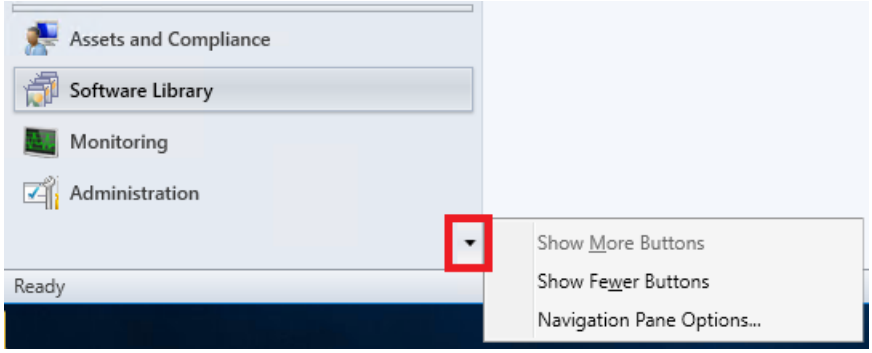
Some areas of the console may not be visible depending on your assigned security role. For more information about roles, see Fundamentals of role-based administration.

Workspaces

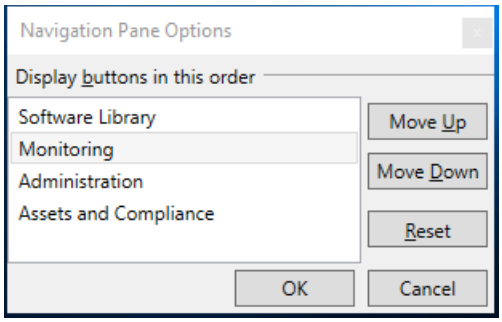
The Configuration Manager console has four **workspaces**:

- **Assets and Compliance**

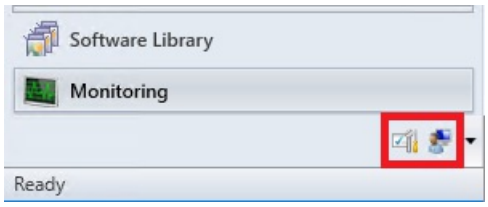
- **Software Library**
- **Monitoring**
- **Administration**



Reorder workspace buttons by selecting the down arrow and choosing **Navigation Pane Options**. Select an item to **Move Up** or **Move Down**. Select **Reset** to restore the default button order.



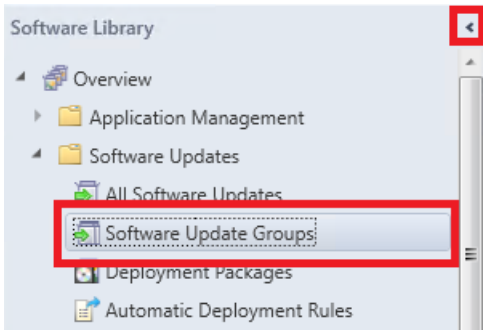
Minimize a workspace button by selecting **Show Fewer Buttons**. The last workspace in the list is minimized first. Select a minimized button and choose **Show More Buttons** to restore the button to its original size.



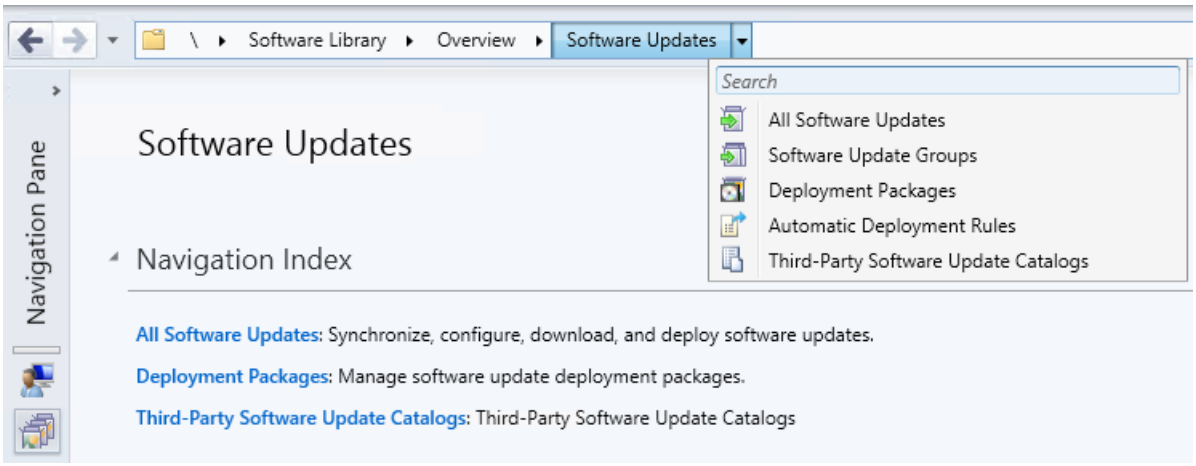
Nodes

Workspaces are a collection of **nodes**. One example of a node is the **Software Update Groups** node in the **Software Library** workspace.

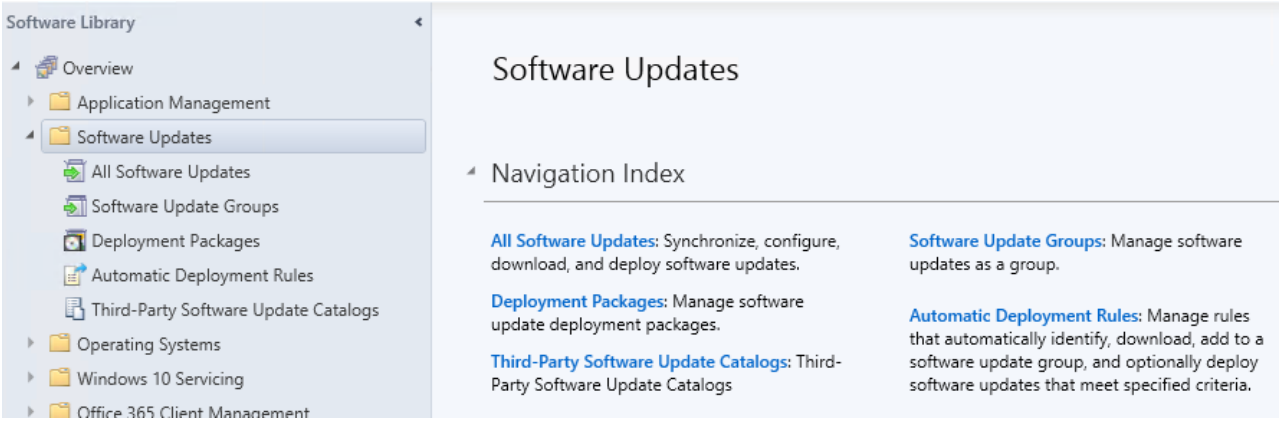
Once you are in the node, you can select the arrow to minimize the navigation pane.



Use the **navigation bar** to move around the console when you minimize the navigation pane.

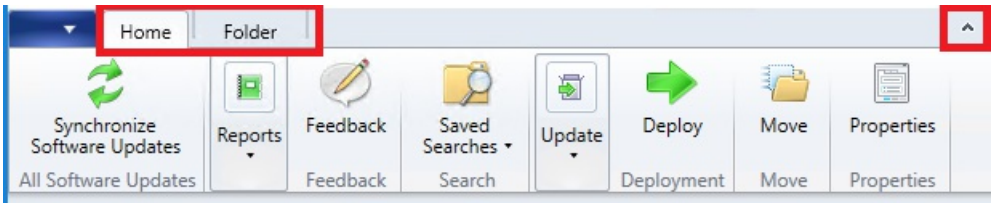


In the console, nodes are sometimes organized into folders. When you select the folder, it usually displays a **navigation index** or a **dashboard**.



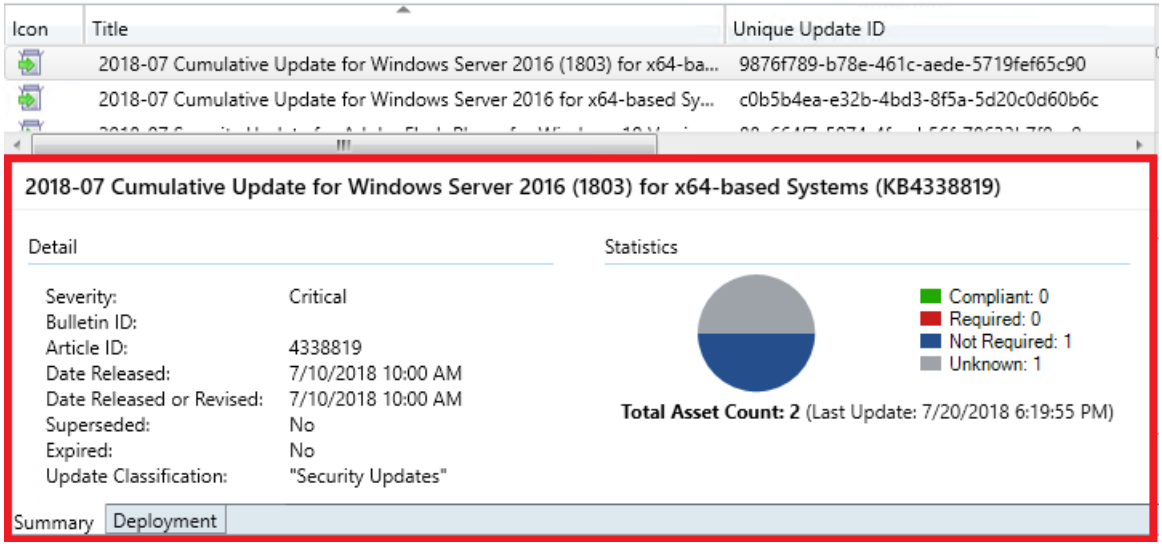
Ribbon

The ribbon is at the top of the Configuration Manager console. The ribbon can have more than one tab and can be minimized using the arrow on the right. The buttons on the ribbon change based on the node. Most of the buttons in the ribbon are also available on context menus.



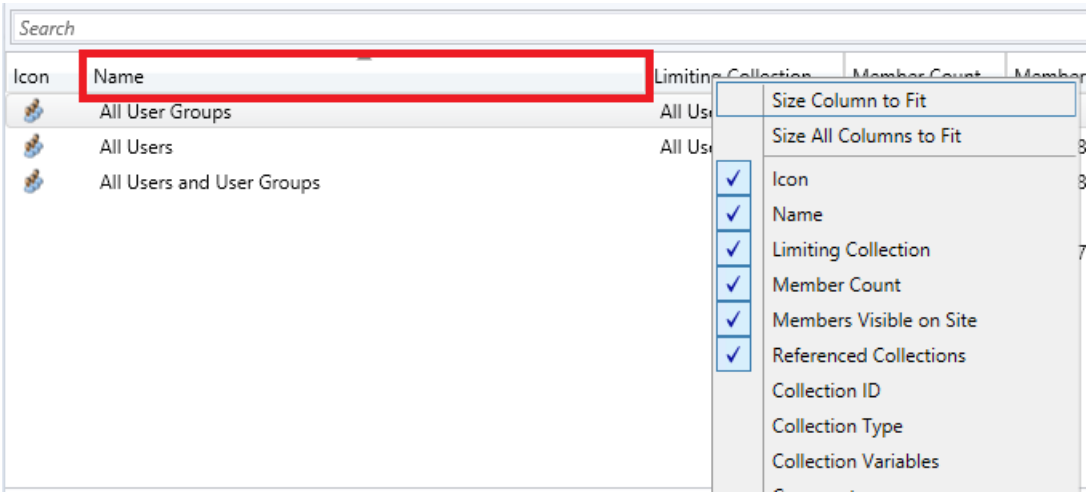
Details pane

You can get additional information about items by reviewing the details pane. The details pane can have one or more tabs. The tabs vary depending on the node.

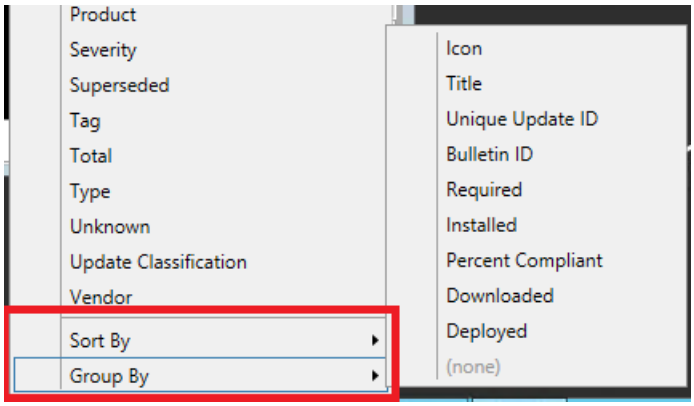


Columns

You can add, remove, reorder, and resize columns. These actions allow you to display the data you prefer. Available columns vary depending on the node. To add or remove a column from your view, right-click on an existing column heading and select an item. Reorder columns by dragging the column heading where you would like it to be.



At the bottom of the column context menu, you can sort or group by a column. Additionally, you can sort by a column by selecting its header.



View recently connected consoles

Starting in version 1902, you can view the most recent connections for the Configuration Manager console. The view includes active connections and those connections that recently connected. You'll always see your current console connection in the list and you only see connections from the Configuration Manager console. You won't see PowerShell or other SDK-based connections to the SMS Provider. The site removes instances from the list that

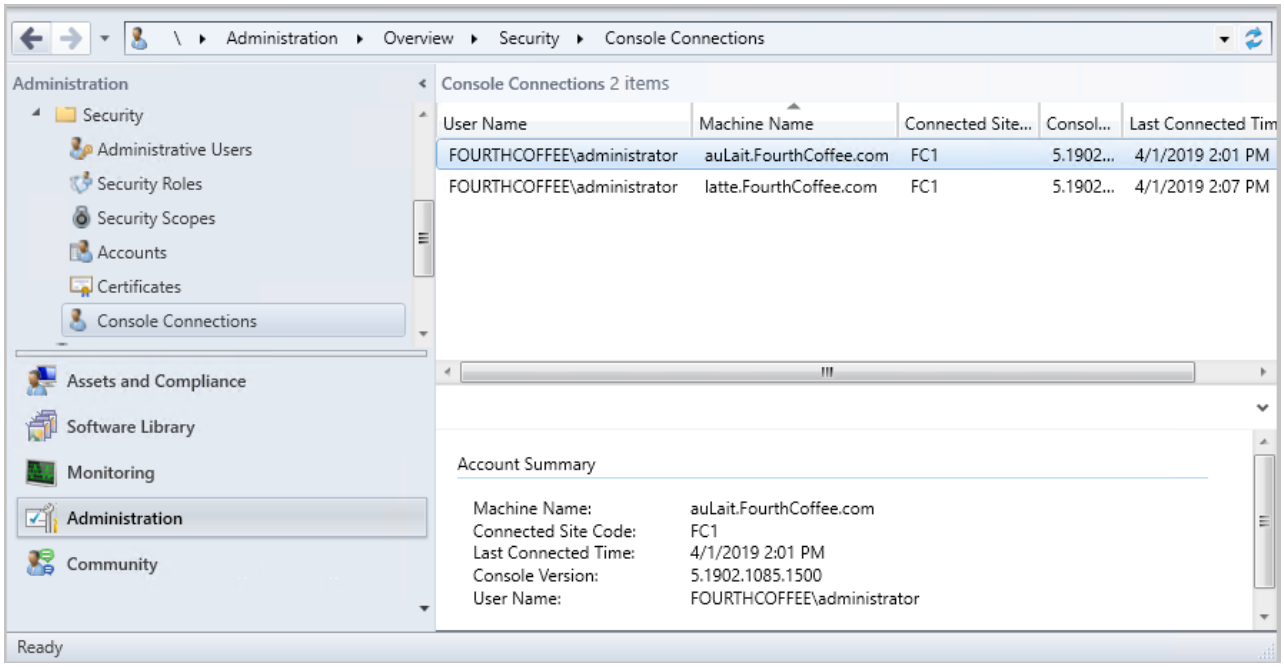
are older than 30 days.

Prerequisites to view connected consoles

- Your account needs the **Read** permission on the **SMS_Site** object
- Install IIS on the SMS Provider server
- Enable the SMS Provider to use a certificate. Use one of the following options:
  - Enable Enhanced HTTP (recommended)
  - Manually bind a PKI-based certificate to port 443 in IIS on the server that hosts the SMS Provider role

View connected consoles

1. In the Configuration Manager console, go to the **Administration** workspace.
2. Expand **Security** and select the **Console Connections** node.
3. View the recent connections, with the following properties:
   - User name
   - Machine name
   - Connected site code
   - Console version
   - Last connected time: When the user last *opened* the console

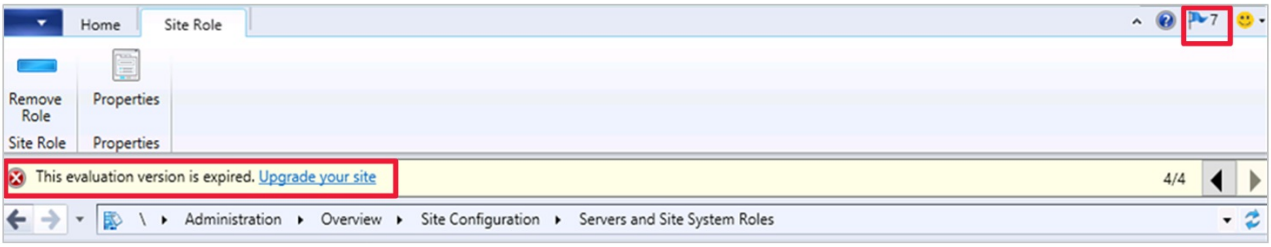


Configuration Manager console notifications

Starting in Configuration Manager version 1902, the console notifies you for the following events:

- When an update is available for Configuration Manager itself
- When lifecycle and maintenance events occur in the environment

This notification is a bar at the top of the console window below the ribbon. It replaces the previous experience when Configuration Manager updates are available. These in-console notifications still display critical information, but don't interfere with your work in the console. You can't dismiss critical notifications. The console displays all notifications in a new notification area of the title bar.



Configure a site to show non-critical notifications

You can configure each site to show non-critical notifications in the properties of the site.

1. In the **Administration** workspace, expand **Site Configuration**, then select the **Sites** node.
2. Select the site you want to configure for non-critical notifications.
3. In the ribbon, select **Properties**.
4. On the **Alerts** tab, select the option to **Enable console notifications for non-critical site health changes**.
   - If you enable this setting, all console users see critical, warning, and information notifications. This setting is enabled by default.
   - If you disable this setting, console users only see critical notifications.

Most console notifications are per session. The console evaluates queries when a user launches it. To see changes in the notifications, restart the console. If a user dismisses a non-critical notification, it notifies again when the console restarts if it's still applicable.

The following notifications reevaluate every five minutes:

- Site is in maintenance mode
- Site is in recovery mode
- Site is in upgrade mode

Notifications follow the permissions of role-based administration. For example, if a user doesn't have permissions to see Configuration Manager updates, they won't see those notifications.

Some notifications have a related action. For example, if the console version doesn't match the site version, select **Install the new console version**. This action launches the console installer.

The following notifications are most applicable to the technical preview branch:

- Evaluation version is within 30 days of expiration (Warning): the current date is within 30 days of the expiration date of the evaluation version
- Evaluation version is expired (Critical): the current date is past the expiration date of the evaluation version
- Console version mismatch (Critical): the console version doesn't match the site version
- Site upgrade is available (Warning): there's a new update package available

For more information and troubleshooting assistance, see the **SmsAdminUI.log** file on the console computer. By default, this log file is at the following path:
`C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\AdminUILog\SmsAdminUI.log`.

In-console documentation dashboard

Starting in Configuration Manager version 1902, there's a **Documentation** node in the new **Community** workspace. This node includes up-to-date information about Configuration Manager documentation and support articles. It includes the following sections:

Product documentation library

- **Recommended**: a manually curated list of important articles.
- **Trending**: the most popular articles for the last month.

- **Recently updated**: articles revised in the last month.

Support articles

- **Troubleshooting articles**: guided walkthroughs to assist with troubleshooting Configuration Manager components and features.
- **New and updated support articles**: articles that are new or updated in the last two months.

Troubleshooting connection errors

The **Documentation** node has no explicit proxy configuration. It uses any OS-defined proxy in the **Internet Options** control panel applet. To retry after a connection error, refresh the **Documentation** node.

Command-line options

The Configuration Manager console has the following command-line options:

OPTION	DESCRIPTION
`/sms:debugview=1`	A DebugView is included in all ResultViews that specify a view. DebugView shows raw properties (names and values).
`/sms:NamespaceView=1`	Shows namespace view in the console.
`/sms:ResetSettings`	The console ignores user-persisted connection and view states. The window size isn't reset.
`/sms:IgnoreExtensions`	Disables any Configuration Manager extensions.
`/sms:NoRestore`	The console ignores previous persisted node navigation.

Tips

General

Role based administration for folders

(Introduced in version 1906)

You can set security scopes on folders. If you have access to an object in the folder but don't have access to the folder, you'll be unable to see the object. Similarly, if you have access to a folder but not an object within it, you won't see that object. Right-click a folder, choose **Set Security Scopes**, then choose the security scopes you want to apply.

Views sort by integer values

(Introduced in version 1902)

We've made improvements to how various views sort data. For example, in the **Deployments** node of the **Monitoring** workspace, the following columns now sort as numbers instead of string values:

- Number Errors
- Number In Progress
- Number Other
- Number Success
- Number Unknown

Move the warning for a large number of results

(Introduced in version 1902)

When you select a node in the console that returns more than 1,000 results, Configuration Manager displays the following warning:

> Configuration Manager returned a large number of results. You can narrow your results by using search. Or, click here to view a maximum of 100000 results.

There's now additional blank space in between this warning and the search field. This move helps to prevent inadvertently selecting the warning to display more results.

Send feedback

(Introduced in version 1806)

Submit product feedback from the console.

- **Send a smile**: Send feedback on what you liked
- **Send a frown**: Send feedback on what you didn't like
- **Send a suggestion**: Takes you to UserVoice to share your idea

For more information, see Product Feedback.

Assets and Compliance workspace

Real-time actions from device lists

(Introduced in version 1906)

There are various ways to display a list of devices under the **Devices** node in the **Assets and Compliance** workspace.

- In the **Assets and Compliance** workspace, select the **Device Collections** node. Select a device collection, and choose the action to **Show members**. This action opens a subnode of the **Devices** node with a device list for that collection.
  - When you select the collection subnode, you can now start **CMPivot** from the Collection group of the ribbon.
- In the **Monitoring** workspace, select the **Deployments** node. Select a deployment, and choose the **View Status** action in the ribbon. In the deployment status pane, double-click the total assets to drill-through to a device list.
  - When you select a device in this list, you can now start **CMPivot** and **Run Scripts** from the Device group of the ribbon.

Collections tab in devices node

(Introduced in version 1906)

In the **Assets and Compliance** workspace, go to the **Devices** node, and select a device. In the details pane, switch to the new **Collections** tab. This tab lists the collections that include this device.

> **NOTE**
>
> - This tab currently isn't available from a devices subnode under the **Device Collections** node. For example, when you select the option to **Show Members** on a collection.
> - This tab may not populate as expected for some users. To see the complete list of collections a device belongs to, you must have the **Full Administrator** security role. This is a known issue.

Add SMBIOS GUID column to device and device collection nodes

(Introduced in version 1906)

In both the **Devices** and **Device Collections** nodes, you can now add a new column for **SMBIOS GUID**. This value is the same as the **BIOS GUID** property of the System Resource class. It's a unique identifier for the device hardware.

Search device views using MAC address

(Introduced in version 1902)

You can search for a MAC address in a device view of the Configuration Manager console. This property is useful for OS deployment administrators while troubleshooting PXE-based deployments. When you view a list of devices, add the **MAC Address** column to the view. Use the search field to add the **MAC Address** search criteria.

View users for a device

Starting in version 1806, the following columns are available in the **Devices** node:

- **Primary user(s)**
- **Currently logged on user**

> **NOTE**
> Viewing the currently logged on user requires user discovery and user device affinity.

For more information on how to show a non-default column, see Columns.

Improvement to device search performance

Starting in version 1806, when searching in a device collection, it doesn't search the keyword against all object properties. When you're not specific about what to search, it searches across the following four properties:

- Name
- Primary user(s)
- Currently logged on user
- Last logon user name

This behavior significantly improves the time it takes to search by name, especially in a large environment. Custom searches by specific criteria are unaffected by this change.

Software Library workspace

Order by program name in task sequence

(Introduced in version 1906)

In the **Software Library** workspace, expand **Operating Systems**, and select the **Task Sequences** node. Edit a task sequence, and select or add the Install Package step. If a package has more than one program, the drop-down list now sorts the programs alphabetically.

Task sequences tab in applications node

(Introduced in version 1906)

In the **Software Library** workspace, expand **Application Management**, go to the **Applications** node, and select an application. In the details pane, switch to the new **Task sequences** tab. This tab lists the task sequences that reference this application.

Drill through required updates

(Introduced in version 1906)

1. Go to one of the following places in the Configuration Manager console:

   - **Software Library** > **Software Updates** > **All Software Updates**
   - **Software Library** > **Windows 10 Servicing** > **All Windows 10 Updates**

- **Software Library** > **Office 365 Client Management** > **Office 365 Updates**

2. Select any update that is required by at least one device.
3. Look at the **Summary** tab and find the pie chart under **Statistics**.
4. Select the **View Required** hyperlink next to the pie chart to drill down into the device list.
5. This action takes you to a temporary node under **Devices** where you can see the devices requiring the update. You can also take actions for the node such as creating a new collection from the list.

Maximize the browse registry window

(Introduced in version 1902)

1. In the **Software Library** workspace, expand **Application Management**, and select the **Applications** node.
2. Select an application that has a deployment type with a detection method. For example, a Windows Installer detection method.
3. In the details pane, switch to the **Deployment Types** tab.
4. Open the properties of a deployment type, and switch to the **Detection Method** tab. Select **Add Clause**.
5. Change the **Setting Type** to **Registry** and select **Browse** to open the **Browse Registry** window. You can now maximize this window.

Edit a task sequence by default

(Introduced in version 1902)

In the **Software Library** workspace, expand **Operating Systems**, and select the **Task Sequences** node. **Edit** is now the default action when opening a task sequence. Previously the default action was **Properties**.

Go to the collection from an application deployment

(Introduced in version 1902)

1. In the **Software Library** workspace, expand **Application Management**, and select the **Applications** node.
2. Select an application. In the details pane, switch to the **Deployments** tab.
3. Select a deployment, and then choose the new **Collection** option in the ribbon on the Deployment tab. This action switches the view to the collection that's the target of the deployment.
   - This action is also available from the right-click context menu on the deployment in this view.

Monitoring workspace

Correct names for client operations

(Introduced in version 1906)

In the **Monitoring** workspace, select **Client Operations**. The operation to **Switch to next Software Update Point** is now properly named.

Show collection name for scripts

(Introduced in version 1906)

In the **Monitoring** workspace, select the **Script Status** node. It now lists the **Collection Name** in addition to the ID.

Remove content from monitoring status

(Introduced in version 1902)

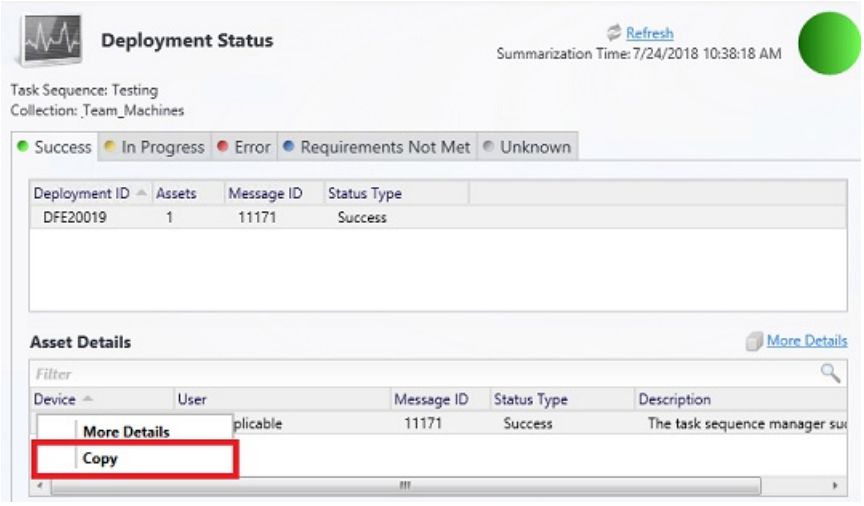
1. In the **Monitoring** workspace, expand **Distribution Status**, and select **Content Status**.
2. Select an item in the list, and choose the **View Status** option in the ribbon.
3. In the Asset Details pane, right-click a distribution point, and select the new option **Remove**. This action removes this content from the selected distribution point.

Copy details in monitoring views

(Introduced in version 1806)

Copy information from the **Asset Details** pane for the following monitoring nodes:

- **Content Distribution Status**
- **Deployment Status**



Administration workspace

Starting in version 1906, you can enable some nodes under the **Security** node to use the administration service. This change allows the console to communicate with the SMS Provider over HTTPS instead of via WMI. For more information, see Administration service.

Next steps

Accessibility features

Accessibility features in Configuration Manager

3/27/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager includes features to help make it accessible for everyone.

> **NOTE**
>
> Starting in version 1902, to improve the accessibility features of the Configuration Manager console, update .NET to version 4.7 or later on the computer running the console.
>
> For more information on the accessibility changes made in .NET 4.7.1 and 4.7.2, see What's new in accessibility in the .NET Framework.

Keyboard shortcuts

Console workspaces

To access a workspace, use the following keyboard shortcuts:

KEYBOARD SHORTCUT	WORKSPACE
Ctrl + 1	Assets and Compliance
Ctrl + 2	Software Library
Ctrl + 3	Monitoring
Ctrl + 4	Administration

Other keyboard shortcuts

KEYBOARD SHORTCUT	PURPOSE
Ctrl + M	Set the focus on the main (central) pane.
Ctrl + T	Set the focus to the top node in the navigation pane. If the focus was already in that pane, the focus is set to the last node you visited.
Ctrl + I	Set the focus to the breadcrumb bar, below the ribbon.
Ctrl + L	Set the focus to the **Search** field, when available.
Ctrl + D	Set the focus to the details pane, when available.
Alt	Change the focus in and out of the ribbon.

Other accessibility features

- To navigate the navigation pane, type the letters of a node name.
- Keyboard navigation through the main view and the ribbon is circular.
- Keyboard navigation in the details pane is circular. To return to the previous object or pane, use Ctrl + D, then Shift + TAB.
- After refreshing a Workspace view, the focus is set to the main pane of that workspace.
- To access a workspace menu, select the Tab key until the Expand/Collapse icon is in focus. Then, select the Down arrow key to access the workspace menu.
- To navigate through a workspace menu, use the arrow keys.
- To access different areas in the workspace, use the Tab key and Shift+Tab keys. To navigate within an area of the workspace, such as the ribbon, use the arrow keys.
- To access the address bar when your focus is in the tree node, use Shift+Tab three times.
- On a wizard or property page, you can move between the boxes with keyboard shortcuts. Select the Alt key plus the underlined character (Alt+_) to select a specific box.
- To navigate to the different nodes of a workspace, enter the first letter of the name of a node. Each key press moves the cursor to the next node that begins with that letter. When you're using a screen reader, the reader reads out the name of that node.

See also

For more information on the fundamentals of navigating Configuration Manager user interfaces, see the following articles:

- Using the Configuration Manager console
- Software Center user guide

> **NOTE**
> The information in this article might apply only to users who license Microsoft products in the United States. If you obtained this product outside of the United States, you can use the subsidiary information card that came with your software package or visit the Microsoft Accessibility website for contact information for Microsoft support services. You can contact your subsidiary to find out whether the type of products and services that are described in this section are available in your area. Information about accessibility is available in other languages, including Japanese and French.

Software Center user guide

7/26/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Your organization's IT admin uses Software Center to install applications, software updates, and upgrade Windows. This user guide explains the functionality of Software Center for users of the computer.

General notes about Software Center functionality:

- This article describes the latest features of Software Center. If your organization is using an older but still supported version of Software Center, not all features are available. For more information, contact your IT admin.
- Your IT admin may disable some aspects of Software Center. Your specific experience may vary.

How to open Software Center

For the simplest method to start Software Center on a Windows 10 computer, press **Start** and type `Software Center`.

If you navigate the Start menu, look under the **Microsoft System Center** group for the **Software Center** icon.

Applications

Select the **Applications** tab to find and install applications that your IT admin deploys to you or this computer.

- **All**: Shows all applications that you can install
- **Required**: Your IT admin enforces these applications. If you uninstall one of these applications, Software Center reinstalls it.
- **Filters**: Your IT admin may create categories of applications. If available, select the drop-down list to filter the view to only those applications in a specific category. Select **All** to show all applications.
- **Sort by**: Rearrange the list of applications. By default this list sorts by **Most recent**. Recently available applications are listed with a **New** tag that is visible for 7 days.
- **Search**: Still can't find what you're looking for? Enter keywords in the Search box to find it!
- **Switch the view**: Select the icons to switch the view between list view and tile view. By default the applications list shows as graphic tiles.
  - Tile view: Your IT admin can customize the icons. Below each tile displays the application name, publisher, and version.
  - List view: This view displays the application icon, name, publisher, version, and status.

Install multiple applications

Install more than one application at a time instead of waiting for one to finish before starting the next. Not all applications qualify:

- The app is visible to you
- The app isn't already downloading or installed
- Your IT admin doesn't require approval to install the app

To install more than one application at a time:

1. To enter multi-select mode in the list view, select the multi-select icon in the upper right corner.

2. Select two or more apps to install by selecting the checkbox to the left of the apps in the list.
3. Select the **Install Selected** button.

The apps install as normal, only now in succession.

Updates

Select the **Updates** tab to view and install software updates that your IT admin deploys to this computer.

- **All**: Shows all updates that you can install
- **Required**: Your IT admin enforces these updates.
- **Sort by**: Rearrange the list of updates. By default this list sorts by **Application name: A to Z**.

To install updates, select **Install All**.

To only install specific updates, select the icon to enter multi-select mode. Check the updates to install, and then select **Install Selected**.

Operating Systems

Select the **Operating Systems** tab to view and install versions of Windows that your IT admin deploys to this computer.

- **All**: Shows all Windows versions that you can install
- **Required**: Your IT admin enforces these upgrades.
- **Sort by**: Rearrange the list of updates. By default this list sorts by **Application name: A to Z**.

Installation status

Select the **Installation status** tab to view the status of applications. You may see the following states:

- **Installed**: Software Center already installed this application on this computer.
- **Downloading**: Software Center is downloading the software to install on this computer.
- **Failed**: Software Center encountered an error in trying to install the software.
- **Scheduled to install after**: Shows the date and time of the device's next maintenance window to install upcoming software. Maintenance windows are defined by your IT admin.
  - The status can be seen in the **All** and the **Upcoming** tab.
  - You can install before the maintenance window time by selecting the **Install Now** button.

Device compliance

Select the **Device compliance** tab to view the compliance status of this computer.

Select **Check compliance** to evaluate this device's settings against the security policies defined by your IT admin.

Options

Select the **Options** tab to view additional settings for this computer.

Work information

Indicate the hours that you typically work. Your IT admin may schedule software installations outside your business hours. Allow at least four hours each day for system maintenance tasks. Your IT admin can still install critical applications and software updates during business hours.

- Select the drop-down lists to select the earliest and latest hours that you use this computer. By default these

values are from **5 AM** through **10 PM**

- Select the checkbox next to the days of the week that you typically use this computer. Software Center only selects the weekdays by default.

Specify whether you regularly use this computer to do your work. Your administrator might automatically install applications or make additional applications available to primary computers.

- Select **I regularly use this computer to do my work** if the computer you're using is a primary computer.

Power management

Your IT admin may set power management policies. These policies help your organization conserve electricity when this computer isn't in use.

To make this computer exempt from these policies, select the checkbox **Do not apply power settings from my IT department to this computer**. This setting is disabled by default; the computer applies power settings.

Computer maintenance

Specify how Software Center applies changes to software before the deadline

- **Automatically install or uninstall required software and restart the computer only outside of the specified business hours**: This setting is disabled by default.
- **Suspend Software Center activities when my computer is in presentation mode**: This setting is enabled by default.
- **Sync Policy**: Select this button when instructed by your IT admin. This computer checks with the servers for anything new, such as applications, software updates, or operating systems.

Custom tab in Software Center

Your IT admin might have added an additional tab to Software Center. This tab is named by your admin and leads to a web site they specify. For instance, you might have a tab called "Help Desk" that leads to your organization's help desk web site.

Fundamentals of System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

If you are new to System Center Configuration Manager, read the fundamental topics to learn about basic concepts for Configuration Manager before you run setup to install your first site. If you are familiar with Configuration Manager, then you can dive right in. We recommend that you start with What's new in System Center Configuration Manager.

For information about supported operating systems and supported environments, hardware requirements, and capacity information, see Supported configurations for System Center Configuration Manager.

When you deploy Configuration Manager, you deploy one or more sites:

- **When you deploy multiple sites**, the sites form child to parent relationships that are collectively referred to as a hierarchy. Use a hierarchy to centrally manage a larger number of sites and devices. Data and information flows down the hierarchy to reach devices that you manage. Information about devices, and results of configuration tasks and requests flow up the hierarchy.
- **When you deploy a single site**, it is also referred to as a hierarchy.

  Some configuration tasks and settings will apply to all sites in a hierarchy, while others apply to individual sites.

Fundamental concepts for System Center Configuration Manager

View the following topics to learn about fundamental concepts for System Center Configuration Manager:

- Fundamentals of sites and hierarchies for System Center Configuration Manager
- Fundamentals of managing devices with System Center Configuration Manager
- Fundamentals of client management tasks for System Center Configuration Manager
- Fundamentals of security for System Center Configuration Manager

Fundamentals of sites and hierarchies for System Center Configuration Manager

2/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

A System Center Configuration Manager deployment must be installed in an Active Directory domain. The foundation of this deployment includes one or more Configuration Manager sites that form a hierarchy of sites. From a single site to a multi-site hierarchy, the type and location of sites you install provide the ability to scale up (expand) your deployment when necessary, and deliver key services to managed users and devices.

Hierarchies of sites

When you install System Center Configuration Manager for the first time, the first Configuration Manager site that you install determines the scope of your hierarchy. The first Configuration Manager site is the foundation from which you will manage devices and users in your enterprise. This first site must be either a central administration site or a stand-alone primary site.

A *central administration site* is suitable for large-scale deployments, provides a central point of administration, and provides the flexibility to support devices that are distributed across a global network infrastructure. After you install a central administration site, you will need to install one or more primary sites as child sites. This configuration is necessary because a central administration site does not directly support management of devices, which is the function of a primary site. A central administration site supports multiple child-primary sites. The child-primary sites are used to directly manage devices, and to control network bandwidth when your managed devices are in different geographical locations.

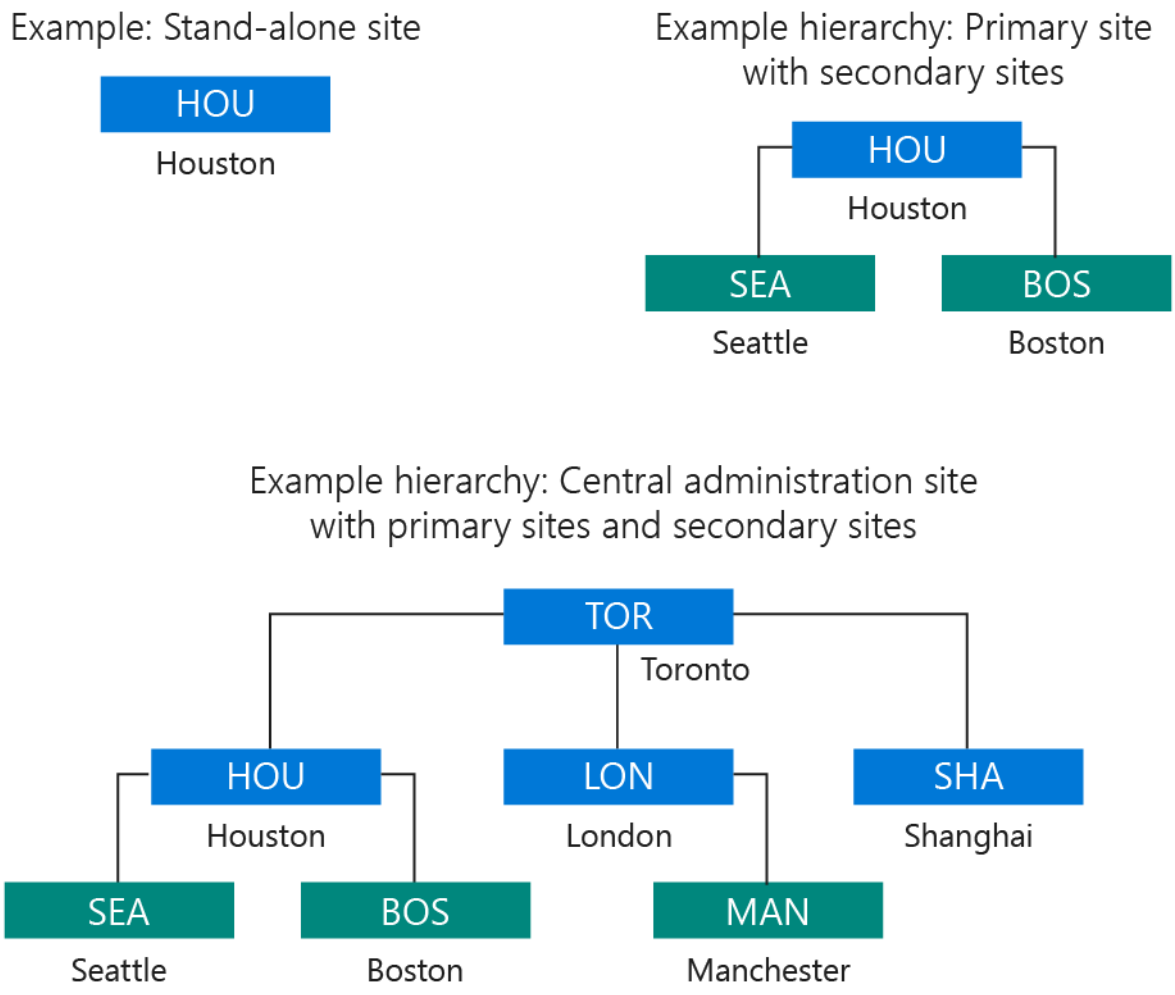
A *stand-alone primary site* is suitable for smaller deployments, and can be used to manage devices without having to install additional sites. Although a stand-alone primary site can limit the size of your deployment, it does support a scenario to expand your hierarchy at a later time by installing a new central administration site. With this site expansion scenario, your stand-alone primary site becomes a child-primary site, and you can then install additional child-primary sites below your new central administration site. You can then expand your initial deployment for future growth of your enterprise.

> **TIP**
> A stand-alone primary site and a child-primary site are really the same type of site: a primary site. The difference in name is based on the hierarchy relationship that is created when you also use a central administration site. This hierarchy relationship can also limit the installation of certain site system roles that extend Configuration Manager functionality. This limitation of roles occurs because certain site system roles can only be installed on the top-tier site of the hierarchy, a central administration site, or a stand-alone primary site.

After you install your first site, you can install additional sites. If your first site was a central administration site, then you can install one or more child-primary sites. After you install a primary site (stand-alone, or child-primary), you can then install one or more secondary sites.

A *secondary site* can only be installed as a child site below a primary site. This site type extends the reach of a primary site to manage devices in locations that have a slow network connection to the primary site. Even though a secondary site extends the primary site, the primary site manages all of the clients. The secondary site provides support for devices in the remote location. It provides support by compressing and then managing the transfer of information across your network that you send (deploy) to clients, and that clients send back to the site.

The following diagrams show some example site designs.



For more information, see the following topics:

- Introduction to System Center Configuration Manager
- Design a hierarchy of sites for System Center Configuration Manager
- Install System Center Configuration Manager sites

Site system servers and site system roles

Each Configuration Manager site installs *site system roles* that support management operations. The following roles are installed by default when you install a site:

- The site server role is assigned to the computer where you install the site.
- The site database server role is assigned to the SQL Server that hosts the site database.

Other site system roles are optional, and are only used when you want to use the functionality that is active in a site system role. Any computer that hosts a site system role is referred to as a site system server.

For a smaller deployment of Configuration Manager, you might initially run all of your site system roles directly on the site server computer. Then, as your managed environment and needs grow, you can install additional site system servers to host additional site system roles to improve the site's efficiency in providing services to more devices.

For information about the different site system roles, see Site system roles in Plan for site system servers and site

system roles for System Center Configuration Manager.

Publishing site information to Active Directory Domain Services

To simplify management of Configuration Manager, you can extend the Active Directory schema to support details that are used by Configuration Manager, and then have sites publish their key information to Active Directory Domain Services (AD DS). Then the computers that you want to manage can securely retrieve site-related information from the trusted source of AD DS. The information clients can retrieve identifies available sites, site system servers, and the services that those site system servers provide.

Extending the Active Directory schema is done only one time for each forest, and can be done before or after you install Configuration Manager. When you extend the schema, you must create a new Active Directory container named System Management in each domain. The container contains a Configuration Manager site that will publish data for clients to find. For more information, see Prepare Active Directory for site publishing.

Publishing site data improves the security of your Configuration Manager hierarchy and reduces administrative overhead, but is not required for basic Configuration Manager functionality.

About upgrade, update, and install for site and hierarchy infrastructure

7/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

When managing System Center Configuration Manager site and hierarchy infrastructure, the terms *upgrade*, *update*, and *install* are used to describe three separate concepts.

Upgrade

Upgrade or *in-place upgrade*, is used when converting your Configuration Manager 2012 site or hierarchy to one that runs System Center Configuration Manager. When you upgrade System Center 2012 Configuration Manager to System Center Configuration Manager, you continue to use the same servers to host your sites and site servers, and you retain your existing data and configurations for Configuration Manager. This is different from Migration which is a way to retain your configurations and data about managed devices while using new System Center Configuration Manager sites installed to new hardware.

For more details, see Upgrade to System Center Configuration Manager.

Update

Update is used for installing in-console updates for System Center Configuration Manager, and for out-of-band updates which are updates that cannot be delivered from within the Configuration Manager console. In-console updates can modify the version of your Current Branch site (or Technical Preview site) so that it runs a higher version. For example, if your site runs version 1806, you can install an update for version 1810. Updates can also install fixes for a known issue, without modifying the site version.

Typically, updates add security fixes, quality improvements, and new features to your existing deployment. If you use the Technical Preview branch, an update can install a newer version of the Technical Preview.

- You choose when to install the in-console update, starting at the top-tier site of your hierarchy.
- You can install any update that is available from within the console. For example, if your site runs version 1802 and both 1806 and 1810 are offered, you should consider installing version 1810 because each version includes the features that were first made available in previously released versions.
- After a new update completes installation at your top-tier site, child primary sites automatically start the process to update. However, you can set Service Windows to control the timing of updates.
- Secondary sites do not automatically install updates. Instead, you manually start the update from within the Configuration Manager console.

For more, see Updates for System Center Configuration Manager, and Technical Preview for System Center Configuration Manager.

Install

Install is used when creating a new Configuration Manager hierarchy from scratch, or adding additional sites to an existing hierarchy.

When you install a new primary site or central administration site, the location of setup.exe and its related source files that you use depends on your installation scenario.

For more, see Prepare to install sites.

Fundamentals of managing devices with Configuration Manager

8/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager can manage two broad categories of devices:

- *Clients* are devices like workstations, laptops, servers, and mobile devices where you install the Configuration Manager client software. Some management functions, like hardware inventory, require this client software.
- *Managed devices* can include *clients*, but typically it's a mobile device where the Configuration Manager client software isn't installed. On this kind of device, you manage by using Intune, or the built-in on-premises mobile device management in Configuration Manager.

  > **IMPORTANT**
  > Hybrid mobile device management is a deprecated feature.

You can also group and identify devices based on the user, not just the client type.

Managing devices with the Configuration Manager client

There are two ways to use the Configuration Manager client software to manage a device. The first way is to discover the device on your network, and then deploy the client software to that device. The other way is to manually install the client software on a new computer, and then have that computer join your site when it joins your network. To discover devices where the client software is not installed, run one or more of the built-in discovery methods. After a device is discovered, use one of several methods to install the client software. For information on using discovery, see Run discovery for Configuration Manager.

After discovering the devices that are supported to run the Configuration Manager client software, you can use one of several methods to install the software. After the software is installed and the client is assigned to a primary site, you can begin to manage the device. Common installation methods include:

- Client push installation
- Software update-based installation
- Group policy
- Manual installation on a computer
- Including the client as part of an OS image that you deploy

After the client is installed, you can simplify the tasks of managing devices by using collections. Collections are groups of devices or users that you create so that you can manage them as a group. For example, you might want to install a mobile device application on all mobile devices that Configuration Manager enrolls. If this is the case, you can use the All Mobile Devices collection.

For more information, see these articles:

- Choose a device management solution

- Client installation methods
- Introduction to collections

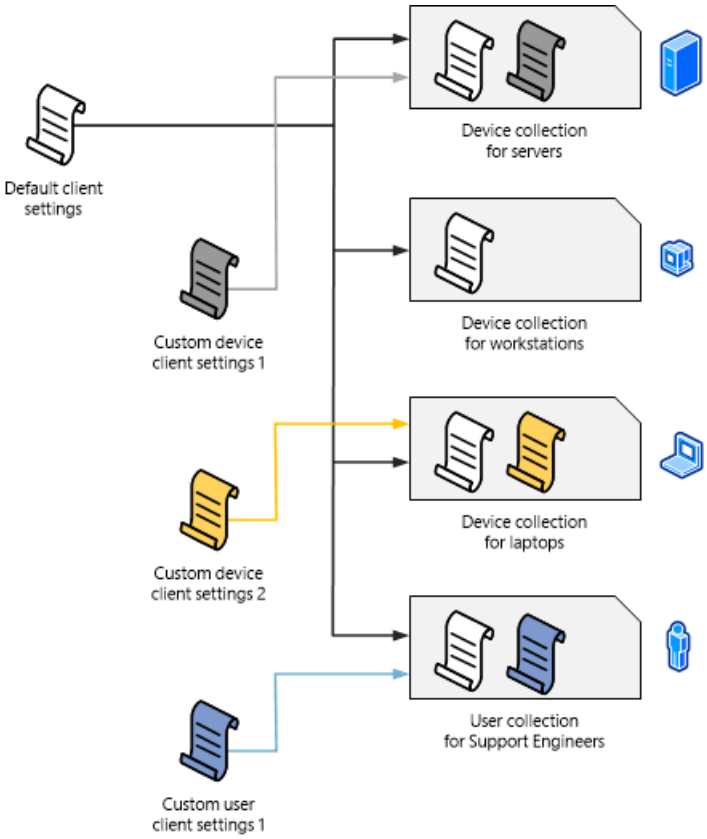
Client settings

When you first install Configuration Manager, all clients in the hierarchy are configured by using the default client settings that you can change. The client settings include these configuration options:

- How frequently the devices communicate with the site.
- Whether the client is set up for software updates and other management operations.
- Whether users can enroll their mobile devices so they're managed by Configuration Manager.

You can create custom client settings and then assign them to collections. Members of the collection are configured to have the custom settings, and you can create multiple custom client settings that are applied in the order that you specify (by numerical order). If there are conflicting settings, the setting that has the lowest order number overrides the other settings.

The following diagram shows an example of how you create and apply custom client settings.



To learn more about client settings, see the following articles:

- How to configure client settings
- About client settings

Managing devices without the Configuration Manager client

Configuration Manager supports the management of some devices that have not installed the client software, and aren't managed by Intune. For more information, see Manage mobile devices with on-premises infrastructure in Configuration Manager and Manage mobile devices with Configuration Manager and Exchange.

User-based management

Configuration Manager supports collections of Azure Active Directory and Active Directory Domain Services users. When you use a user collection, you can install software on all computers that members of the collection use. To make sure that the software you deploy only installs on the devices that are specified as a user's primary device, set up user device affinity. A user can have one or more primary devices.

One of the ways that users can control their software deployment experience is to use the **Software Center** client interface. The **Software Center** is automatically installed on client computers and is run from the Windows **Start** menu. The **Software Center** lets users manage their own software and do the following tasks:

- Install software
- Schedule software to automatically install outside working hours
- Configure when Configuration Manager can install software on a device
- Configure the access settings for remote control, if remote control is set up in Configuration Manager
- Configure options for power management, if an administrator sets up this option
- Browse for, install, and request software
- Configure preference settings
- When it's set up, specify a primary device for user device affinity

For more information, see the following articles:

- Plan for Software Center
- Link users and devices with user device affinity
- Software Center user guide

Fundamentals of client management tasks for System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

After you install the System Center Configuration Manager clients, there are several tasks that you run to manage the clients. Some of the tasks are run from the Configuration Manager console. Other tasks are run from the Configuration Manager client application. The Configuration Manager client application is installed with the Configuration Manager client software.

Configuration Manager console tasks

In the Configuration Manager console, you can perform various client management tasks:

- Deploy applications, software updates, maintenance scripts, and operating systems. Configure installation for a specific date and time, make the software available for users to install when they are requested, or configure applications to be uninstalled.
- Help protect computers from malware and security threats, and notify you when problems are detected.
- Define client configuration settings that you want to monitor, and remediate if they are out of compliance.
- Collect hardware and software inventory information, which includes monitoring and reconciling license information from Microsoft.
- Troubleshoot computers by using remote control.
- Implement power management settings to manage and monitor the power consumption of computers.

The Configuration Manager console monitors the previous tasks in near real time. Notification and status information for each task is available in the Configuration Manager console. To capture data and historical trending, use the integrated reporting capabilities of SQL Server Reporting Services. Clients submit details to the site as client status. Client status information provides data about the health of the client and client activity, and is viewed in the console or by using the built-in reports for Configuration Manager. This data helps identify computers that are not responding and in some cases, problems are automatically remediated.

For more information about management tasks for clients, see How to manage clients in System Center Configuration Manager and How to manage clients for Linux and UNIX servers in System Center Configuration Manager. To learn about using reports, see Introduction to reporting in System Center Configuration Manager.

Configuration Manager client application

When you install the Configuration Manager client software, the Configuration Manager client application is installed too. Unlike Software Center, the Configuration Manager client application is designed for the help desk rather than for the end user. Some configuration options require local administrative permissions, and most options require technical knowledge about how the Configuration Manager client application works. You can use this application to perform the following tasks on a client:

- View properties about the client, such as the build number, its assigned site, the management point it is communicating with, and whether the client is using a public key infrastructure (PKI) certificate or a self-

signed certificate.

- Confirm that the client has successfully downloaded a client policy after the client is installed for the first time. Also confirm that the client settings are enabled or disabled as expected, according to the client settings that are configured in the Configuration Manager console.
- Start client actions. For example, download the client policy if there was a recent configuration change in the Configuration Manager console, and you do not want to wait until the next scheduled time.
- Manually assign a client to a Configuration Manager site or try to find a site. Then specify the Domain Name System (DNS) suffix for management points that publish to DNS.
- Configure the client cache that temporarily stores files. Then delete files in the cache if you require more disk space to install software.
- Configure settings for Internet-based client management.
- View configuration baselines that were deployed to the client, initiate compliance evaluation, and view compliance reports.

Fundamentals of security for Configuration Manager

6/17/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article summarizes the following fundamental security components of any Configuration Manager environment:

- Security layers
- Role-based administration
- Securing client endpoints
- Configuration Manager accounts and groups
- Privacy

Security layers

Security for Configuration Manager consists of the following layers:

- Windows OS and network security
- Network infrastructure: firewalls, intrusion detection, public key infrastructure (PKI)
- Configuration Manager security controls
- SMS Provider
- Site database permissions

Windows OS and network security

The first layer is provided by Windows security features for both the OS and the network. This layer includes the following components:

- File sharing to transfer files between Configuration Manager components
- Access Control Lists (ACLs) to help secure files and registry keys
- Internet Protocol Security (IPsec) to help secure communications
- Group Policy to set security policy
- Distributed Component Object Model (DCOM) permissions for distributed applications, like the Configuration Manager console
- Active Directory Domain Services to store security principals
- Windows account security, including some groups that Configuration Manager creates during setup

Network infrastructure

Additional security components, like firewalls and intrusion detection, help provide defense for the whole environment. Certificates issued by industry standard public key infrastructure (PKI) implementations help provide authentication, signing, and encryption.

Configuration Manager security controls

In addition to security provided by the Windows server and network infrastructure, Configuration Manager controls access to its console and resources in several ways. By default, only local administrators have rights to the files and registry keys that the Configuration Manager console requires on computers where you install it.

SMS Provider

The next layer of security is based on access through Windows Management Instrumentation (WMI), specifically the SMS Provider. The SMS Provider is a Configuration Manager component that grants a user access to query the site database for information. By default, access to the provider is restricted to members of the local SMS Admins group. This group at first contains only the user who installed Configuration Manager. To grant other accounts permission to the Common Information Model (CIM) repository and the SMS Provider, add the other accounts to the SMS Admins group.

Starting in version 1810, you can specify the minimum authentication level for administrators to access Configuration Manager sites. This feature enforces administrators to sign in to Windows with the required level.

For more information, see Plan for the SMS Provider.

Site database permissions

The final layer of security is based on permissions to objects in the site database. By default, the Local System account and the user account that you used to install Configuration Manager can administer all objects in the site database. Grant and restrict permissions to additional administrative users in the Configuration Manager console by using role-based administration.

Role-based administration

Configuration Manager uses role-based administration to help secure objects like collections, deployments, and sites. This administration model centrally defines and manages hierarchy-wide security access settings for all sites and site settings.

An administrator assigns *security roles* to administrative users and group permissions. The permissions are connected to different Configuration Manager object types, for example, to create or change client settings.

Security scopes group specific instances of objects that an administrative user is responsible to manage, like an application that installs Microsoft Office.

The combination of security roles, security scopes, and collections define the objects that an administrative user can view and manage. Configuration Manager installs some default security roles for typical management tasks. Create your own security roles to support your specific business requirements.

For more information, see Configure role-based administration.

Securing client endpoints

Configuration Manager secures client communication to site system roles by using either self-signed or PKI certificates, or Azure Active Directory (Azure AD) tokens. Some scenarios require the use of PKI certificates. For example, internet-based client management, and for mobile device clients.

You can configure the site system roles to which clients connect for either HTTPS or HTTP client communication. Client computers always communicate by using the most secure method that's available. Client computers only fall back to using the less secure communication method if you have site systems roles that allow HTTP communication.

For more information, see Plan for security.

Configuration Manager accounts and groups

Configuration Manager uses the Local System account for most site operations. Some management tasks might require you to create and maintain additional accounts. Configuration Manager creates several default groups and SQL Server roles during setup. You might have to manually add computer or user accounts to the default groups and SQL Server roles.

For more information, see Accounts used in Configuration Manager.

Privacy

Before you implement Configuration Manager, consider your privacy requirements. Although enterprise management products offer many advantages because they can effectively manage lots of clients, this software might affect the privacy of users in your organization. Configuration Manager includes many tools to collect data and monitor devices. Some tools might raise privacy concerns in your organization.

For example, when you install the Configuration Manager client, it enables many management settings by default. This configuration causes the client software to send information to the Configuration Manager site. The site stores client information in the site database. The client information isn't directly sent to Microsoft. For more information, see Diagnostics and usage data.

See also

- Plan for security
- Security and privacy for Configuration Manager clients
- Configure security
- Communication between endpoints
- Cryptographic controls technical reference

Fundamentals of role-based administration for System Center Configuration Manager

7/26/2019 • 7 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

With System Center Configuration Manager, you use role-based administration to secure the access that is needed to administer Configuration Manager. You also secure access to the objects that you manage, like collections, deployments, and sites. After you understand the concepts introduced in this article, you can Configure role-based administration for System Center Configuration Manager.

The role-based administration model centrally defines and manages hierarchy-wide security access settings for all sites and site settings by using the following items:

- *Security roles* are assigned to administrative users to provide those users (or groups of users) permission to different Configuration Manager objects. For example, permission to create or change client settings.
- *Security scopes* are used to group specific instances of objects that an administrative user is responsible to manage, like an application that installs Microsoft Office 2010.
- *Collections* are used to specify groups of user and device resources that the administrative user can manage.

  With the combination of security roles, security scopes, and collections, you segregate the administrative assignments that meet your organization's requirements. Used together, they define the administrative scope of a user, which is what that user can view and manage in your Configuration Manager deployment.

Benefits of role-based administration

- Sites aren't used as administrative boundaries.
- You create administrative users for a hierarchy and only need to assign security to them one time.
- All security assignments are replicated and available throughout the hierarchy.
- There are built-in security roles that are used to assign the typical administration tasks. Create your own custom security roles to support your specific business requirements.
- Administrative users see only the objects that they have permissions to manage.
- You can audit administrative security actions.

When you design and implement administrative security for Configuration Manager, you use the following to create an *administrative scope* for an administrative user:

- Security roles
- Collections
- Security scopes

The administrative scope controls the objects that an administrative user views in the Configuration Manager console, and it controls the permissions that a user has on those objects. Role-based administration configurations replicate to each site in the hierarchy as global data, and then are applied to all administrative connections.

IMPORTANT

Intersite replication delays can prevent a site from receiving changes for role-based administration. For information about how to monitor intersite database replication, see the Data transfers between sites in System Center Configuration Manager topic.

Security roles

Use security roles to grant security permissions to administrative users. Security roles are groups of security permissions that you assign to administrative users so that they can perform their administrative tasks. These security permissions define the administrative actions that an administrative user can perform and the permissions that are granted for particular object types. As a security best practice, assign the security roles that provide the least permissions.

Configuration Manager has several built-in security roles to support typical groupings of administrative tasks, and you can create your own custom security roles to support your specific business requirements. Examples of the built-in security roles:

- *Full Administrator* grants all permissions in Configuration Manager.
- *Asset Manager* grants permissions to manage the Asset Intelligence Synchronization Point, Asset Intelligence reporting classes, software inventory, hardware inventory, and metering rules.
- *Software Update Manager* grants permissions to define and deploy software updates. Administrative users who are associated with this role can create collections, software update groups, deployments, and templates.
- *Security Administrator* grants permissions to add and remove administrative users and associate administrative users with security roles, collections, and security scopes. Administrative users who are associated with this role can also create, modify, and delete security roles and their assigned security scopes and collections.

TIP

You can view the list of built-in security roles and custom security roles you create, including their descriptions, in the Configuration Manager console. To view the roles, in the **Administration** workspace, expand **Security**, and then select **Security Roles**.

Each security role has specific permissions for different object types. For example, the *Application Author* security role has the following permissions for applications: Approve, Create, Delete, Modify, Modify Folder, Move Object, Read, Run Report, and Set Security Scope.

You can't change the permissions for the built-in security roles, but you can copy the role, make changes, and then save these changes as a new custom security role. You can also import security roles that you've exported from another hierarchy, for example, from a test network. Review the security roles and their permissions to determine whether you'll use the built-in security roles, or whether you have to create your own custom security roles.

To help you plan for security roles

1. Identify the tasks that the administrative users perform in Configuration Manager. These tasks might relate to one or more groups of management tasks, such as deploying applications and packages, deploying operating systems and settings for compliance, configuring sites and security, auditing, remotely controlling computers, and collecting inventory data.
2. Map these administrative tasks to one or more of the built-in security roles.

3. If some of the administrative users perform the tasks of multiple security roles, assign the multiple security roles to these administrative users instead of creating a new security role that combines the tasks.

4. If the tasks that you identified don't map to the built-in security roles, create and test new security roles.

For information about how to create and configure security roles for role-based administration, see Create custom security roles and Configure security roles in the Configure role-based administration for System Center Configuration Manager article.

Collections

Collections specify the user and computer resources that an administrative user can view or manage. For example, for administrative users to deploy applications or to run remote control, they must be assigned to a security role that grants access to a collection that contains these resources. You can select collections of users or devices.

For more information about collections, see Introduction to collections in System Center Configuration Manager.

Before you configure role-based administration, check whether you have to create new collections for any of the following reasons:

- Functional organization. For example, separate collections of servers and workstations.
- Geographic alignment. For example, separate collections for North America and Europe.
- Security requirements and business processes. For example, separate collections for production and test computers.
- Organization alignment. For example, separate collections for each business unit.

For information about how to configure collections for role-based administration, see Configure collections to manage security in the Configure role-based administration for System Center Configuration Manager article.

Security scopes

Use security scopes to provide administrative users with access to securable objects. A security scope is a named set of securable objects that are assigned to administrator users as a group. All securable objects must be assigned to one or more security scopes. Configuration Manager has two built-in security scopes:

- The *All* built-in security scope grants access to all scopes. You can't assign objects to this security scope.
- The *Default* built-in security scope is used for all objects, by default. When you first install Configuration Manager, all objects are assigned to this security scope.

If you want to restrict the objects that administrative users can see and manage, you must create and use your own custom security scopes. Security scopes don't support a hierarchical structure and can't be nested. Security scopes can contain one or more object types, which include the following items:

- Alert subscriptions
- Applications
- Boot images
- Boundary groups
- Configuration items
- Custom client settings
- Distribution points and distribution point groups
- Driver packages
- Folders (starting in version 1906)
- Global conditions
- Migration jobs

- Operating system images
- Operating system installation packages
- Packages
- Queries
- Sites
- Software metering rules
- Software update groups
- Software updates packages
- Task sequence packages
- Windows CE device setting items and packages

There are also some objects that you can't include in security scopes because they're only secured by security roles. Administrative access to these objects can't be limited to a subset of the available objects. For example, you might have an administrative user who creates boundary groups that are used for a specific site. Because the boundary object doesn't support security scopes, you can't assign this user a security scope that provides access to only the boundaries that might be associated with that site. Because a boundary object can't be associated to a security scope, when you assign a security role that includes access to boundary objects to a user, that user can access every boundary in the hierarchy.

Objects that aren't limited by security scopes include the following items:

- Active Directory forests
- Administrative users
- Alerts
- Antimalware policies
- Boundaries
- Computer associations
- Default client settings
- Deployment templates
- Device drivers
- Exchange Server connector
- Migration site-to-site mappings
- Mobile device enrollment profiles
- Security roles
- Security scopes
- Site addresses
- Site system roles
- Software titles
- Software updates
- Status messages
- User device affinities

Create security scopes when you have to limit access to separate instances of objects. For example:

- You have a group of administrative users who must be able to see production applications and not test applications. Create one security scope for production applications and another for the test applications.
- Different administrative users require different access for some instances of an object type. For example, one group of administrative users requires Read permission to specific software update groups, and another group of administrative users requires Modify and Delete permissions for other software update groups. Create different security scopes for these software update groups.

For information about how to configure security scopes for role-based administration, see the Configure security scopes for an object in the Configure role-based administration for System Center Configuration Manager article.

Next steps

Configure role-based administration for System Center Configuration Manager

Introduction to the long-term servicing branch of Configuration Manager

8/28/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Long-Term Servicing Branch)

The long-term servicing branch (LTSB) of Configuration Manager is a distinct branch that's designed as an install option available to all customers. However, it's the only option for customers who let lapse their Software Assurance (SA) or equivalent subscription rights for Configuration Manager.

Based on Configuration Manager version 1606, the LTSB has reduced functionality when compared to the current branch of Configuration Manager.

> **TIP**
> The Configuration Manager LTSB isn't related to the System Center suite long-term servicing channel (LTSC). For more information, see Overview of System Center release options.

Features that aren't available

The current branch of Configuration Manager supports the following functionality that isn't available when you use the LTSB:

- In-console updates that add new features and improvements.
- Support for newly released operating systems to use as site servers and clients.
- Use of a Microsoft Intune subscription to support:
  - Intune in a hybrid mobile device management (MDM) configuration
  - On-premises MDM
- The Windows 10 servicing dashboard and servicing plans, including support for recent Windows 10 versions.
- Support for future releases of Windows Server and Windows 10 LTSB
- Asset Intelligence
- Cloud-based distribution points
- Exchange Online as an Exchange Connector

Although support for these features isn't available with the LTSB, some features remain visible in the Configuration Manager console, but can't be selected or used.

Cloud integrations, as well as any features included with Configuration Manager current branch version 1610 or later, aren't available to the LTSB. These features include, but aren't limited to the following:

- Co-management
- Desktop Analytics
- Cloud management gateway
- Azure Active Directory integration
- Apps from the Microsoft Store for Business

Find LTSB documentation

The LTSB is based on current branch version 1606. Use the current branch documentation, with caveats and

limitations that are specific to the LTSB. Those caveats and limitations are identified in the following articles:

- Install the LTSB
- Upgrade the LTSB to the current branch
- Supported configurations for the LTSB
- Manage the LTSB of Configuration Manager

When you reference current branch documentation for the LTSB, details that apply to version 1606 or earlier also apply to the LTSB. Features or details that are introduced with version 1610 or later aren't supported by the LTSB.

Licensing overview for the LTSB

Customers with active Software Assurance (SA) on System Center Configuration Manager licenses, or with equivalent subscription rights as of October 1, 2016, have rights to use the October 2016 version 1606 release of System Center Configuration Manager. Customers with rights to System Center Configuration Manager on or after October 1, 2016, will find two licensed options upon installation: Current Branch and Long-Term Servicing Branch (LTSB).

Customers that have perpetual rights to System Center Configuration Manager, or that allow SA or subscription to lapse after October 1, can install the version of System Center Configuration Manager LTSB that is current at the time of lapse.

For more information about these licenses, see the Complete terms and conditions for the products you purchase through Microsoft Volume Licensing programs.

For more information about licensing for Configuration Manager branches, see Configuration Manager licensing and branches.

Next Steps

If you decide that the Configuration Manager LTSB is the correct branch for your environment, install a new LTSB site as part of a new hierarchy, or upgrade a System Center 2012 Configuration Manager site and hierarchy.

Supported Configurations for the Long-Term Servicing Branch of System Center Configuration Manager

9/11/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Long-Term Servicing Branch)

Use the information in this topic to understand what operating systems and product dependencies are supported by the Long-Term Servicing Branch (LTSB) of Configuration Manager. If not stated otherwise in this or the LTSB specific topics, the same configurations and limitations that apply to the Current Branch version 1606 apply to the LTSB. When conflicts occur, use the information that applies to the edition you are using. Typically, the LTSB is more limited than the Current Branch.

General statement of support

The following products and technologies are supported by this branch of Configuration Manager. However, their inclusion in this content does not express an extension of support for any product or version beyond that product's individual support lifecycle. Products that are beyond their support lifecycle are not supported for use with Configuration Manager. For more information, visit the Microsoft Support Lifecycle website and read the Microsoft Support Lifecycle Policy FAQ.

Additionally, products and product versions that are not listed in the following topics are not supported unless they have been announced on the Enterprise Mobility + Security Blog.

Limitations for future support: The LTSB has limited support for future server and client operating systems and product dependencies. The platforms list for the LTSB is fixed for the life of the release:

Windows:

- Only quality and security updates for Windows are supported.
- No support is added for current branches (CB), current branches for business (CBB), or LTSB of Windows 10.
- No support for new major versions of Windows Server.

SQL Server:

- Only quality and security updates, or minor upgrades like service packs, is supported for SQL Server.
- No support for new major versions of SQL Server.

Site systems and servers

The LTSB supports the use of the following Windows computer operating systems as site systems. Each operating system has the same requirements and limitations as the same entry in Supported operating systems for site system servers. For example, the Server Core installation of Windows 2012 R2 must be an x64 version, is only supported to host a distribution point, and does not support PXE or Multicast.

Supported operating systems:

- Windows Server 2016
- Windows Server 2012 R2 (x64): Standard, Datacenter
- Windows Server 2012 (x64): Standard, Datacenter

- Windows Server 2008 R2 with SP1 (x64): Standard, Enterprise, Datacenter
- Windows Server 2008 with SP2 (x86, x64): Standard, Enterprise, Datacenter *(See note 1)*
- Windows 10 Enterprise 2015 LTSB (x86, x64)
- Windows 10 Enterprise 2016 LTSB (x86, x64)
- Windows 8.1 (x86, x64): Professional, Enterprise
- Windows 7 with SP1 (x86, x64): Professional, Enterprise, Ultimate
- The Server Core installation of Windows Server 2012
- The Server Core installation of Windows Server 2012 R2

Note 1: This operating system is not supported for site servers or site system roles with the exception of the distribution point and pull-distribution point. You can continue to use this operating system as a distribution point until deprecation of this support is announced, or this operating system's extended support period expires. For more information, see Installation of System Center Configuration Manager CB and LTSB fails on Windows Server 2008.

Client management

The following sections identify the client operating systems that you can manage with the LTSB. The LTSB does not support the addition of new operating systems as supported clients.

Windows computers

You can use the LTSB to manage the following Windows computer operating systems with the Configuration Manager client software that is included with Configuration Manager. For more information, see How to deploy clients to Windows computers in System Center Configuration Manager.

Supported operating systems:

- Windows Server 2016
- Windows Server 2012 R2 (x64): Standard, Datacenter (Note 1)
- Windows Server 2012 (x64): Standard, Datacenter (Note 1)
- Windows Storage Server 2012 R2 (x64)
- Windows Storage Server 2012 (x64)
- Windows Server 2008 R2 with SP1 (x64): Standard, Enterprise, Datacenter (Note 1)
- Windows Storage Server 2008 R2 (x86, x64): Workgroup, Standard, Enterprise
- Windows Server 2008 with SP2 (x86, x64): Standard, Enterprise, Datacenter (Note 1)
- Windows 10 Enterprise 2015 LTSB (x86, x64)
- Windows 10 Enterprise 2016 LTSB (x86, x64)
- Windows 8.1 (x86, x64): Professional, Enterprise
- Windows 7 with SP1 (x86, x64): Professional, Enterprise, Ultimate
- The Server Core installation of Windows Server 2012 R2 (x64) (Note 2)
- The Server Core installation of Windows Server 2012 (x64) (Note 2)
- The Server Core installation of Windows Server 2008 R2 SP1 (x64)
- The Server Core installation of Windows Server 2008 SP2 (x86, x64)

(Note 1) Datacenter releases are supported but not certified for Configuration Manager.
(Note 2) To support client push installation, the computer that runs this operating system version must run the File Server role service for the File and Storage Services server role. For information about installing Windows features on a Server Core computer, see Install Server Roles and Features on a Server Core Server in the Windows Server 2012 TechNet library.

Windows Embedded

You can use the LTSB to manage the following Windows Embedded devices by installing the client software on the

device. For more information, see Planning for client deployment to Windows Embedded devices in System Center Configuration Manager.

Requirements and limitations:

- All client features are supported on supported Windows Embedded systems that do not have write filters enabled.
- Clients that use one of the following are supported for all features except power management:
  - Enhanced Write Filters (EWF)
  - RAM File-Based Write Filters (FBWF)
  - Unified Write Filters (UWF)
- The Application Catalog is not supported for any Windows Embedded device.
- Before you can monitor detected malware on Windows Embedded devices based on Windows XP, you must install the Microsoft Windows WMI scripting package on the embedded device. Use Windows Embedded Target Designer to install this package. The *WBEMDISP.DLL* and *WBEMDISP.TLB* files must exist and be registered in the %windir%\System32\WBEM folder on the embedded device to ensure that detected malware is reported.

Supported operating systems:

- Windows 10 Enterprise 2016 LTSB (x86, x64)
- Windows 10 Enterprise 2015 LTSB (x86, x64)
- Windows Embedded 8.1 Industry (x86, x64)
- Windows Thin PC (x86, x64)
- Windows Embedded POSReady 7 (x86, x64)
- Windows Embedded Standard 7 with SP1 (x86, x64)
- Windows Embedded POSReady 2009 (x86)
- Windows Embedded Standard 2009 (x86)

Windows CE

You can manage Windows CE devices with the Configuration Manager mobile device legacy client that is included with Configuration Manager.

Requirements and limitations:

- The mobile device client requires 0.78 MB of storage space to install the client. A mobile device can require up to 256 KB of additional storage space to sign in.
- Features for these mobile devices vary by platform and client type. For information about the kind of management functions that Configuration Manager supports for a mobile device legacy client, see Choose a device management solution for System Center Configuration Manager.

Supported operating systems:

- Windows CE 7.0 (ARM and x86 processors)

Supported languages include:

- Chinese (simplified and traditional)
- English (US)
- French (France)
- German

- Italian
- Japanese
- Korean
- Portuguese (Brazil)
- Russian
- Spanish (Spain)

Mac computers

You can use the LTSB to manage Mac OS X computers with the Configuration Manager client for Mac.

The Mac client installation package is not supplied with the Configuration Manager media. You can download it as part of the "Clients for Additional Operating Systems" download from the Microsoft Download Center.

Support for Mac operating systems is limited to those listed in this section. Support does not include additional operating systems that might be supported by a future update to Mac client installation packages for Current Branch.

For more information, see How to deploy clients to Macs in System Center Configuration Manager.

Supported versions:

- Mac OS X 10.9 (Mavericks)
- Mac OS X 10.10 (Yosemite)
- Mac OS X 10.11 (El Capitan)

Linux and UNIX servers

You can use the LTSB to manage Linux and UNIX servers with the Configuration Manager client for Linux and UNIX.

The Linux and UNIX client installation packages are not supplied with the Configuration Manager media. You can download them as part of the "Clients for Additional Operating Systems" download from the Microsoft Download Center. In addition to client installation packages, the client download includes the install script that manages the installation of the client on each computer.

Support for Linux and UNIX operating systems is limited to those listed in this section. Support does not include additional operating systems that might be supported by a future update to Linux and UNIX client packages for Current Branch.

Requirements and limitations:

- To review operating system file dependencies for the client for Linux and UNIX, see Prerequisites for Client Deployment to Linux and UNIX Servers.
- For an overview of the management capabilities supported for computers that run Linux or UNIX, see How to deploy clients to UNIX and Linux servers in System Center Configuration Manager.
- For supported versions of Linux and UNIX, the listed version includes all subsequent minor versions. For example, where support is indicated for CentOS version 6, this also includes any subsequent minor version of CentOS 6, such as CentOS 6.3. Similarly, when support is listed for an operating system that uses service packs, such as SUSE Linux Enterprise Server 11 SP1, support includes subsequent service packs for that operating system version.
- For information about client installation packages and the Universal Agent, see How to deploy clients to UNIX and Linux servers in System Center Configuration Manager.

Supported versions:

The following versions are supported by using the indicated .tar file.

AIX

VERSION	FILE
Version 5.3 (Power)	ccm-Aix53ppc.<build>.tar
Version 6.1 (Power)	ccm-Aix61ppc.<build>.tar
Version 7.1 (Power)	ccm-Aix71ppc.<build>.tar

CentOS

VERSION	FILE
Version 5 x86	ccm-Universalx86.<build>.tar
Version 5 x64	ccm-Universalx64.<build>.tar
Version 6 x86	ccm-Universalx86.<build>.tar
Version 6 x64	ccm-Universalx64.<build>.tar
Version 7 x64	ccm-Universalx64.<build>.tar

Debian

VERSION	FILE
Version 5 x86	ccm-Universalx86.<build>.tar
Version 5 x64	ccm-Universalx64.<build>.tar
Version 6x86	ccm-Universalx86.<build>.tar
Version 6 x64	ccm-Universalx64.<build>.tar
Version 7 x86	ccm-Universalx86.<build>.tar
Version 7 x64	ccm-Universalx64.<build>.tar
Version 8 x86	ccm-Universalx86.<build>.tar
Version 8 x64	ccm-Universalx64.<build>.tar

HP-UX

VERSION	FILE
Version 11iv2 IA64	ccm-HpuxB.11.23i64.<build>.tar
Version 11iv2 PA-RISC	ccm-HpuxB.11.23PA.<build>.tar
Version 11iv3 IA64	ccm-HpuxB.11.31i64.<build>.tar

VERSION	FILE
Version 11iv3 PA-RISC	ccm-HpuxB.11.31PA.<build>.tar

Oracle Linux

VERSION	FILE
Version 5 x86	ccm-Universalx86.<build>.tar
Version 5 x64	ccm-Universalx64.<build>.tar
Version 6 x86	ccm-Universalx86.<build>.tar
Version 6 x64	ccm-Universalx64.<build>.tar
Version 7 x64	ccm-Universalx64.<build>.tar

Red Hat Enterprise Linux (RHEL)

VERSION	FILE
Version 4 x86	ccm-RHEL4x86.<build>.tar
Version 4 x64	ccm-RHEL4x64.<build>.tar
Version 5 x86	ccm-Universalx86.<build>.tar
Version 5 x64	ccm-Universalx64.<build>.tar
Version 6 x86	ccm-Universalx86.<build>.tar
Version 6 x64	ccm-Universalx64.<build>.tar
Version 7 x64	ccm-Universalx64.<build>.tar

Solaris

VERSION	FILE
Version 9 SPARC	ccm-Sol9sparc.<build>.tar
Version 10 x86	ccm-Sol10x86.<build>.tar
Version 10 SPARC	ccm-Sol10sparc.<build>.tar
Version 11 x86	ccm-Sol11x86.<build>.tar
Version 11 SPARC	ccm-Sol11sparc.<build>.tar

SUSE Linux Enterprise Server (SLES)

VERSION	FILE
Version 9 x86	ccm-SLES9x86.<build>.tar
Version 10 SP1 x86	ccm-Universalx86.<build>.tar
Version 10 SP1 x64	ccm-Universalx64.<build>.tar
Version 11 SP1 x86	ccm-Universalx86.<build>.tar
Version 11 SP1 x64	ccm-Universalx64.<build>.tar
Version 12 x64	ccm-Universalx64.<build>.tar

Ubuntu

VERSION	FILE
Version 10.04 LTS x86	ccm-Universalx86.<build>.tar
Version 10.04 LTS x64	ccm-Universalx64.<build>.tar
Version 12.04 LTS x86	ccm-Universalx86.<build>.tar
Version 12.04 LTS x64	ccm-Universalx64.<build>.tar
Version 14.04 LTS x86	ccm-Universalx86.<build>.tar
Version 14.04 LTS x64	ccm-Universalx64.<build>.tar

Exchange Server connector

The LTSB supports limited management of devices that connect to your Exchange Server instance, without installing client software. For more information, see Manage mobile devices with System Center Configuration Manager and Exchange.

Requirements and limitations:

- Configuration Manager offers limited management for mobile devices. Limited management is available when you use the Exchange Server connector for Exchange Active Sync (EAS) capable devices that connect to a server running Exchange Server or Exchange Online.
- For more information about the management functions that Configuration Manager supports for mobile devices that the Exchange Server connector manages, see Choose a device management solution for System Center Configuration Manager.

Supported versions of Exchange Server:

- Exchange Server 2010 SP1
- Exchange Server 2010 SP2
- Exchange Server 2013

> **NOTE**
> The LTSB does not support the management of devices that connect through an online service, like Exchange Online (Office 365).

Configuration Manager console

The LTSB supports the following operating systems to run the Configuration Manager console. Each computer that hosts the console must have a minimum .NET Framework version of 4.5.2 except for Windows 10, which requires a minimum of .NET Framework 4.6.

Supported operating systems:

- Windows Server 2016
- Windows Server 2012 R2 (x64): Standard, Datacenter
- Windows Server 2012 (x64): Standard, Datacenter
- Windows Server 2008 R2 with SP1 (x64): Standard, Enterprise, Datacenter
- Windows Server 2008 with SP2 (x86, x64): Standard, Enterprise, Datacenter
- Windows 10 Enterprise 2016 LTSB (x86, x64)
- Windows 10 Enterprise 2015 LTSB (x86, x64)
- Windows 8.1 (x86, x64): Professional, Enterprise
- Windows 7 with SP1 (x86, x64): Professional, Enterprise, Ultimate

SQL Server versions supported for the site database and reporting point

The LTSB supports the following versions of SQL Server to host the site database and reporting point. For each supported version, the same configuration requirements and limitations that appear in Support for SQL Server versions for the Current Branch apply to the LTSB. This includes the use of a SQL Server Cluster, or a SQL Server AlwaysOn availability group.

Supported versions:

- SQL Server 2016: Standard, Enterprise
- SQL Server 2014 SP2: Standard, Enterprise
- SQL Server 2014 SP1: Standard, Enterprise
- SQL Server 2012 SP3: Standard, Enterprise
- SQL Server 2008 R2 SP3: Standard, Enterprise, Datacenter
- SQL Server 2016 Express
- SQL Server 2014 Express SP2
- SQL Server 2014 Express SP1
- SQL Server 2012 Express SP3

Support for Active Directory domains

All LTSB site systems must be members of a supported Windows Active Directory domain. Support for Active Directory domains has the same requirements and limitations as those that appear in Support for Active Directory domains, but is limited to the following domain functional levels:

Supported levels:

- Windows Server 2008

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Additional support topics that apply to the Long-Term Servicing Branch

The information in the following Current Branch topics apply to the LTSB:

- Size and scale numbers
- Site and site system prerequisites
- High availability options
- Recommended hardware
- Support for Windows features and networks
- Support for virtualization environments

Install and upgrade with the version 1606 baseline media for System Center Configuration Manager

7/19/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch), (Long-Term Servicing Branch)

When you run Setup from the version 1606 baseline media for Configuration Manager, you can install the Long-Term Servicing Branch or a Current branch site of System Center Configuration Manager.

The baseline media is available on DVD as part of Microsoft System Center 2016, or from System Center Configuration Manager (Current Branch and Long-Term Servicing Branch 1606) release. To learn about baseline media, see Baseline and update versions.

When you use the version 1606 baseline media, the site you install or upgrade to is:

- A *Current Branch site* that is equivalent to a site that was first installed using the 1511 baseline media, and then updated to version 1606 plus the 1606 hotfix rollup - KB3186654.
- An *LTSB site* that is equivalent to the Current Branch site that runs version 1606 plus the 1606 hotfix rollup - KB3186654. The baseline media already includes the hotfix rollup. But, the LTSB does not support all of the features or capabilities available with the Current Branch, as detailed in Introduction to the Long-Term Servicing Branch of System Center Configuration Manager.

If you are not familiar with the different branches of System Center Configuration Manager, see Which branch of Configuration Manager should I use.

Changes to Setup with the 1606 baseline media

The 1606 baseline media introduces the following changes to Setup for Configuration Manager.

Branch and edition

When you run Setup, you are now presented with a Licensing page where you can select the branch of Configuration Manager you want to install. You can choose either the Current Branch or LTSB as a licensed installation, or you can choose an Evaluation edition of the Current Branch as a non-licensed installation.

For more information, see Licensing and branches for System Center Configuration Manager.

Software Assurance expiration

During Setup, you have the option to enter the **Software Assurance expiration date** value. This is an optional value that you can specify as a convenient reminder.

> **NOTE**
> Microsoft does not validate the expiration date you enter and will not use this date for license validation. Instead, you can use it as a reminder of your expiration date. This is useful because Configuration Manager periodically checks for new software updates offered online, and your software assurance license status should be current to be eligible to use these additional updates.

- You can specify the date value on the **Product Key** page of the Setup Wizard when you run Setup from the System Center Configuration Manager version 1606 baseline media.
- You can also specify this date by selecting **Hierarchy Settings Properties** > **Licensing** in the Configuration Manager console.

For more information, see "Software Assurance agreements" in Licensing and branches for System Center Configuration Manager.

Additional pre-upgrade configurations

Prior to starting an upgrade of System Center 2012 Configuration Manager to the LTSB, you must take the following additional steps as part of pre-upgrade checklist.
Uninstall the site system roles that the LTSB does not support:

- Asset Intelligence synchronization point
- Microsoft Intune connector
- Cloud-based distribution points

For more information, see Upgrade to System Center Configuration Manager.

New scripted installation options

The version 1606 baseline media supports a new unattended script file key for scripted installations of a new top-level site. This applies to installing a new stand-alone primary site or adding a central administration site as part of a site expansion scenario.

When using an unattended script to install a licensed branch, you must add the following section, key names, and values to the Options section of your script. You don't need to use these values to script the install of an Evaluation edition of the Current Branch:

SABranchOptions

- **Key Name: SAActive**
  - Values: 0 or 1.
  - Details: 0 installs a non-licensed Evaluation edition of Current Branch, and 1 installs a licensed edition.
- **CurrentBranch**
  - Values: 0 or 1.
  - Details: 0 installs the Long-Term Servicing Branch, and 1 installs the Current Branch.

For example, to install a licensed Current Branch edition you would use:

Key Name: SABranchOptions

- **SAActive = 1**
- **CurrentBranch = 1**

> **IMPORTANT**
>
> **SABranchOptions** only works with Setup from the baseline media. It does not apply when you run Setup from the CD.Latest folder of a site you previously installed using the version 1606 baseline media.
>
> **SABranchOptions** does not apply to scripted upgrades from System Center 2012 Configuration Manager and always results in the Current Branch.

For more information, see Use a command line to install System Center Configuration Manager sites.

Install a new site

When you use the 1606 baseline media to install a new site of either branch, use the site planning, preparation, and installation procedures documented in the Installing System Center Configuration Manager sites topic with the addition of the following considerations for Setup:

- During Setup you must choose the branch of Configuration Manager that you want to install, and you can specify details for your Software Assurance agreement.
- All sites in the same hierarchy must run the same branch. It is not supported to have a hierarchy with a mix of LTSB and Current Branch at different sites.
- New scripted installation. For more information, see "New scripted installation options" earlier in this article.

Expand a stand-alone primary site

You can expand a stand-alone primary site that runs the LTSB. The process is no different than that used for a Current Branch site with one caveat:

- When installing the new central administration site you must use Setup from the original source media you used to install the LTSB site. Running Setup from the CD.Latest folder for this scenario is not supported.

For more information about expanding a site, see "Expand a stand-alone primary site" in Install a site using the Setup Wizard.

Upgrade from System Center 2012 Configuration Manager

When you upgrade from System Center 2012 Configuration Manager, use the site planning, preparation, and procedures as documented in the Upgrade to System Center Configuration Manager topic, but with the following changes:

Upgrade to the Current Branch:

- During Setup, you must choose the Current Branch, and you can specify details for your Software Assurance agreement.
- New scripted installation. For more information, see "New scripted installation options" earlier in this article.

Upgrade to the LTSB:

- Additional steps to following in the pre-upgrade checklist.
- During Setup you must choose the LTSB, and you can specify details for your Software Assurance agreement.
- You can only upgrade a site that runs System Center 2012 Configuration Manager with Service Pack 1, System Center 2012 Configuration Manager with Service Pack 2, System Center 2012 R2 Configuration Manager with Service Pack 1, or System Center 2012 R2 Configuration Manager with no service pack.

In-place upgrade paths for the 1606 baseline media

You can use the 1606 baseline media to upgrade the following to a licensed edition of System Center Configuration Manager:

- System Center 2012 R2 Configuration Manager with Service Pack 1
- System Center 2012 R2 Configuration Manager with no service pack (this requires the use of the baseline media for version 1606 that was rereleased on December 15th, 2016.)
- System Center 2012 Configuration Manager with Service Pack 2
- System Center 2012 Configuration Manager with Service Pack 1 (this requires the use of the baseline media for version 1606 that was rereleased on December 15th, 2016.)

You can also use this media to upgrade a non-licensed Evaluation edition of Current Branch to a fully licensed version of the Current Branch.

This media does not support the upgrade of:

- Other versions of System Center 2012 Configuration Manager.
- Configuration Manager 2007 or earlier.
- A release candidate installation of System Center Configuration Manager.

About the CD.Latest folder and the LTSB

The following are limitations on using the media that Configuration Manager creates in the CD.Latest folder on the site server. These limits apply to sites that run the LTSB:

Media in the CD.Latest folder is supported for:

- Site recovery.
- Site maintenance.
- Installing additional child primary sites.

Media in the CD.Latest folder is not supported for:

- Installing a central administration site as part of a site expansion scenario.

For more information, see the CD.Latest folder.

Backup, recovery, and site maintenance for the LTSB

To back up, recover, or run site maintenance on a site that runs the LTSB, use the guidance and procedures from Backup and recovery for System Center Configuration Manager.

Use Configuration Manager Setup from the CD.Latest folder of the backup of your LTSB site.

Manage the Long Term Servicing Branch of Configuration Manager

6/18/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Long-Term Servicing Branch)

When you use the Long-Term Servicing Branch (LTSB) of System Center Configuration Manager, the following can help you understand important changes that affect how you manage your infrastructure.

Because the LTSB is equivalent to Current Branch version 1606 (with some exceptions like Intune integration and cloud-related features), most tasks you use for planning, deployment, configuration, and day-to-day management are the same.

For example, the LTSB supports the same number of sites, site types, clients, and general infrastructure as the Current Branch. Therefore, you use the guidance found in the site and hierarchy planning and design topics for the Current Branch. Similarly, for features with the LTSB that are supported by both branches, like Software Updates or Operating System Deployment, use the guidance found in those sections of the Current Branch documentation with the caveats of not having access to feature changes introduced after version 1606 of the Current Branch.

The following sections provide information about manage tasks that are not similar.

Updates and servicing

Only critical security updates are made available as in-console updates in the LTSB.

Information about regular updates for the subsequent Current Branch releases are visible in the console, but are not made available to the LTSB. They are not downloaded and cannot be installed.

To support in-console updates for critical security fixes, an LTSB site requires the use of the service connection point. You can configure this site system role in offline or online mode, as is done for the Current Branch. The LTSB collects and submits the same telemetry and usage data as the Current Branch.

The LTSB supports the use of the Hotfix Installer and the Update Registration tool, as documented for the Current Branch.

For general information about updates and servicing, see Updates for Configuration Manager.

Changes for site expansion and the CD.Latest folder

When you run the LTSB and are expanding a stand-alone primary site by installing a new central administration site, you must use Setup and the source files from the version 1606 baseline media. For the Current Branch, you run Setup and use source files from the CD.Latest folder.

Although you do not run Setup for site expansion from the CD.Latest folder, you continue to use the CD.Latest folder for site recovery, and to install a new child primary site when your first LTSB site was a central administration site.

For more information about site expansion, see Expand a stand-alone primary site. For more information about the CD.Latest folder, see The CD.Latest folder.

Recovery

When you recover a site, you must restore the site or site database to its original branch. You cannot recover a

Current Branch site database to a LTSB installation, or vice versa.

Upgrade the long-term servicing branch to the current branch

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Long-Term Servicing Branch)

Use this topic to learn how to upgrade (convert) a site and hierarchy that runs the Long-Term Servicing Branch (LTSB) of Configuration Manager to the Current Branch.

When you have a current Software Assurance agreement (or similar licensing rights) that grants you rights to use the Current Branch, you can convert your installation from the LTSB to the Current Branch. This is a one-way conversion because there is no support for converting a Current Branch site to the LTSB.

If you have multiple sites, you only need to convert the top-tier site of your hierarchy. After the top-tier site is converted:

- Child primary sites automatically convert.
- You must manually update secondary sites from within the Configuration Manager console.

Run setup to convert the Long-Term Servicing Branch

On the top-tier site of your hierarchy, you can run Configuration Manager setup from qualifying baseline media and select **Site maintenance**. Then, when presented with the licensing page, select the option for the Current Branch and complete the wizard.

When your site has converted to the Current Branch, previously unavailable features and capabilities will be available for use.

> **NOTE**
> Qualifying baseline media is a media that has a version that is equal to or later than your LTSB installation.

For example, because the LTSB is based on version 1606, you cannot use the baseline 1511 media to convert to the Current Branch. Instead, you run setup from the same version 1606 baseline media that you used to install the LTSB site, and choose the licensing option for the Current Branch. Alternately, if a later baseline of the Current Branch has been released, you can run setup from that baseline media.

For a list of baseline versions, see **Baseline and update versions** in Updates for Configuration Manager.

Use the Configuration Manager console to convert the long-term servicing branch

If your site runs the LTSB, you can use the following option in the Configuration Manager console to convert to the Current Branch:

1. In the console, go to **Administration** > **Site Configuration** > **Sites**, and then open **Hierarchy Settings**.
2. In **Hierarchy Settings**, switch to the **Licensing** tab. Select the option to **Convert to Current Branch**, and then choose **Apply**.

When your site has converted to the Current Branch, previously unavailable features and capabilities will be

available for use.

Which branch of Configuration Manager should I use?

7/9/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch, Long-Term Servicing Branch, and Technical Preview)

There are three branches of System Center Configuration Manager available: current branch, long-term servicing branch, and technical preview branch. Use this topic to help choose the right branch for you.

> **TIP**
> All sites in a hierarchy must run the same branch. It isn't supported to have a hierarchy with different branches at different sites.

Current branch

This branch is licensed for use in a production environment. Use this branch to get the latest features and functionalities. If you have one of the following licenses, you can use this branch:

- System Center Datacenter
- System Center Standard
- System Center Configuration Manager
- Equivalent subscription rights

For more information about Software Assurance and licensing options, see Licensing and branches for System Center Configuration Manager and Frequently asked questions for Configuration Manager branches and licensing.

Microsoft plans to release updates for System Center Configuration Manager current branch a few times per year. For versions of Configuration Manager released prior to 1710, support is for 12 months. Beginning with the 1710 release, each update version remains in support for 18 months from its general availability (GA) release date. Technical support is provided for the entire period of support. However, our support structure is dynamic, evolving into two distinct servicing phases that depend on the availability of the latest current branch version. (For more information, review the topic titled Support for System Center Configuration Manager current branch versions. Updates to newer versions are available as in-console updates.

To install the Current Branch as a new site, use baseline media. Also use baseline media to upgrade from System Center 2012 Configuration Manager with Service Pack 2 or System Center 2012 R2 Configuration Manager with Service Pack 1. Access to this media depends on how your organization licensed System Center Configuration Manager.

You can also use the baseline media to install a new site that is an evaluation edition of the current branch. The evaluation edition doesn't require a license. You can use the evaluation edition for 180 days. It supports upgrade to a licensed edition of the current branch. To install only an evaluation edition, get it from the TechNet Evaluation Center.

> **NOTE**
>
> Use baseline media to install sites for a new Configuration Manager hierarchy. If you previously installed a baseline version, use in-console updates to update your sites to a new version.
>
> Sites that are updated using in-console updates result in sites that are the same as the new site installed using the baseline media.
>
> For more information, see Updates for System Center Configuration Manager.

Features of the current branch

- Receives in-console updates that make new features available for use.
- Receives in-console updates that deliver security and quality fixes to existing features.
- Supports out-of-band updates when necessary. For more information, see Use the update registration tool or Use the hotfix installer.
- Integrates with Microsoft Intune and other cloud-based services.
- Supports migration of data to and from other Configuration Manager installations.
- Supports upgrade from previous versions of Configuration Manager.
- Supports installation as an evaluation edition, from which you can later upgrade to a fully licensed installation.

The initial release of the Current Branch was version 1511. Subsequent updates include versions 1602, 1606, and so on. Each version remains in support for one year, and Microsoft recommends that you update to the newest version soon after its release. You can wait up to one year before updating to a newer version, and you can also skip an update to install the newest version available. Because each version is cumulative, if you skip over an update and install the newest version, you still get access to all features and improvements from previous versions.

For more information, see Support for current branch versions.

Update options

- With active Software Assurance, you can install in-console updates for current branch versions.
- There is no option to convert the current branch to a technical preview branch. Technical preview branches are separate installations that don't require a license.
- There is no option to convert your current branch to the long-term servicing branch (LTSB). You must uninstall the current branch and then install the LTSB as a new installation.

Long-term servicing branch

This branch is licensed for use in production for Configuration Manager customers who are using the current branch and have allowed their Configuration Manager Software Assurance (SA) or equivalent subscription rights to expire after October 1, 2016. For more about Software Assurance and licensing options, see Licensing and branches for System Center Configuration Manager and Frequently asked questions for Configuration Manager branches and licensing.

The LTSB is based on version 1606. This branch doesn't receive in-console updates that deliver new features or update existing capabilities. However, critical security fixes are provided. To install the LTSB, you must use the version 1606 baseline media that you get with System Center 2016. Later baseline versions don't support install of the LTSB.

To install the LTSB as a new site or as an upgrade from a supported Configuration Manager 2012 site, use the version 1606 baseline media that you get with System Center 2016. You can use baseline media to install a new site that runs version 1606 of the current branch, or a new site that runs the long-term servicing branch.

TIP

To learn about System Center 2016, see System Center 2016 documentation. This documentation also identifies how to get System Center 2016, which requires a Microsoft license agreement or similar rights.

To find System Center Configuration Manager version 1606 in the Volume Licensing Service Center (VLSC), go to the **Downloads and Keys** tab of the VLSC, search for `System Center 2016`, and then select either **System Center 2016 Datacenter** or **System Center 2016 Standard**.

You can also get an evaluation edition of System Center 2016 from the TechNet Evaluation Center.

Features of the LTSB

- Receives in-console updates that deliver critical security fixes.
- Provides an installation option when your SA agreement or equivalent rights to Configuration Manager have expired.
- Supports upgrade (conversion) to the current branch when you have a current SA agreement or equivalent rights to Configuration Manager.

Limitations

The LTSB is based on the current branch version 1606 and has the following limitations:

- The LTSB is supported for 10 years of critical security updates after its general availability (October 2016), after which, support for this branch expires. For more information about the support lifecycle, see Microsoft Lifecycle Policy.
- Supports a limited set list of server and client operating systems and related technologies, like SQL Server versions. For more about what is supported with this branch, see Supported configurations for the long-term servicing branch.
- Doesn't receive updates for new features
- Doesn't support the following capabilities:
  - Adding a Microsoft Intune subscription, which prevents the use of:
    - Intune in a hybrid MDM configuration
    - On-premises MDM
  - The Windows 10 servicing dashboard, servicing plans, or Windows 10 semi-annual channel
  - Future releases of Windows 10 LTSB and Windows Server
  - Asset intelligence
  - Cloud-based distribution points
  - Exchange Online as an Exchange Connector
  - Any pre-release features

Update options

- You can convert your LTSB install to a current branch installation. Conversion to the current branch is supported before or after support for the LTSB expires.

  To convert, you must have an active Software Assurance agreement with Microsoft. For more information, see the following links:

  - Upgrade the Long-Term Servicing Branch to the Current Branch
  - Licensing and branches for System Center Configuration Manager
  - Baseline and update versions
- There is no option to convert the LTSB to a technical preview branch. Technical preview branches are separate installations that don't require a license.
- You can't upgrade an evaluation edition of the current branch to an LTSB installation.

Technical preview branch

The technical preview branch is for use in a lab environment. Learn about and try out the newest features being developed for Configuration Manager. It isn't supported in a production environment, and doesn't require you to have a Software Assurance license agreement.

To install a new site that runs the technical preview branch, use the latest baseline media for the technical preview branch. After you install the technical preview branch, new versions are available as in-console updates each month.

Features of the technical preview branch

- Based on recent baseline versions of the current branch
- Receives in-console updates that update your installation to the latest technical preview branch version
- Includes new features that are being developed, and for which Microsoft wants your feedback
- Receives updates that apply only to the technical preview branch

Limitations

- Support is limited, including only a single primary site and up to 10 clients.
- Can't be upgraded to a current branch or LTSB.
- Doesn't support the following behaviors:
  - Using migration to import or export data to another Configuration Manager installation
  - Upgrade from a previous version of Configuration Manager
  - Installation as an evaluation edition

Features that are first introduced in a technical preview branch are often added to the current branch in a later update. Each new technical preview branch version includes the features from previous technical preview branches, even after those features have been added to the current branch.

For more information, see the Technical preview for System Center Configuration Manager.

Update options

- You can install any in-console update for a new technical preview branch version.
- There is no option to convert a technical preview branch to the current branch or LTSB.

Identify your version and branch

Version

To check the version of your site, in the console go to **About System Center Configuration Manager** at the upper-left corner of the console. This dialog displays the **Site version**. For a list of site versions, see Baseline and update versions.

Branch

To confirm the branch of your site, in the console go to **Administration** > **Site Configuration** > **Sites**, and open **Hierarchy Settings**. If there is an option to convert to the current branch and it is active, the site runs the LTSB version. When the site runs the current branch, this option is grayed out.

For more information about the different versions of Configuration Manager, see Baseline and update versions.

Configuration Manager and Windows as a Service

2/12/2019 • 2 minutes to read • Edit Online

Applies To: System Center Configuration Manager (Current Branch)

System Center Configuration Manager provides comprehensive control over feature updates for Windows 10. To fully adopt the Windows as a service model, you also must adopt the Configuration Manager current branch model. To stay current with Windows 10, requires that you stay current with Configuration Manager for the best experience. New versions of Configuration Manager are required to take full advantage of the exciting new enterprise features for Windows 10. This article is intended to be a landing page for the key articles required to adopt Configuration Manager current branch. Configuration Manager current branch gets you on your way to Windows as a service.

Key articles about adopting Configuration Manager current branch

ARTICLE	DESCRIPTION
Overview of Configuration Manager current branch	Provides a brief summary of the key points for the new servicing model for Configuration Manager (Current Branch)
Support lifecycle	Explains the new support and servicing model.
Removed and deprecated items	Provides early notice about future changes that might affect your use of Configuration Manager.
Updates to Configuration Manager current branch	Explains the easy in-console method of applying feature updates to Configuration Manager.
Get available updates	Explains the two modes available to get new Configuration Manager feature updates.
Update checklist	Provides update version-specific checklists, if applicable.
Install new Configuration Manager feature updates	Explains the simple installation steps for feature updates.
Support for Windows 10	Provides a support matrix for Windows 10 (and ADK) versions.
Technical Previews for Configuration Manager	Provides information about the ConfigMgr technical preview program.

Key articles about adopting Windows as a service

ARTICLE	DESCRIPTION
Manage Windows as a service	Explains how to use servicing plans to deploy Windows 10 feature updates.
Upgrade Windows 10 via task sequence	The details of creating a task sequence to upgrade Windows 10 with additional recommendations.

ARTICLE	DESCRIPTION
Phased deployments	Phased deployments automate a coordinated, sequenced rollout of a task sequence across multiple collections.
Optimize Windows 10 update delivery	Use Configuration Manager to manage update content to stay current with Windows 10.
Integrate with Upgrade Readiness	Upgrade Readiness allows you to assess and analyze the readiness of devices in your environment for an upgrade to Windows 10.
Windows Update for Business integration (optional)	Explains how to define and deploy Windows Update for Business (WUfB) policies using Configuration Manager.
Use co-management with Microsoft Intune and Windows Update for Business (optional)	Provides an overview of co-management

Related articles

- In-place upgrade to System Center Configuration Manager (Current Branch) from ConfigMgr 2012
- Plan for migration to System Center Configuration Manager (Current Branch) from ConfigMgr 2007

Use the Configuration Manager client software for extended interoperability with future versions of a Current Branch site

8/28/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Business requirements might not allow you to regularly update the Configuration Manager client on some devices. For example, you need to follow change management policies, or the device is mission-critical. Accommodate these needs by installing a new client for long-term use, called the extended interoperability client (EIC). Only use the EIC for specific devices that can't be frequently updated, like kiosk or point-of-sale devices. Continue to use automatic client upgrade for most of your clients.

How it works

Typically, when you install a new in-console update for Configuration Manager, clients automatically update their client software so they can use those new features. With this scenario, you still update to the current branch receiving the new features and updates. Most devices update the Configuration Manager client software with each version update you install. However, on a subset of critical systems that you don't want to receive client software updates, you install the extended interoperability client. These clients don't install new client software until you explicitly deploy a new version of the client software to them.

Supported versions

The following table lists the versions of the Configuration Manager client that are supported for this scenario:

VERSION	AVAILABILITY DATE	SUPPORT END DATE
1902 5.00.8790	March 27, 2019	No earlier than March 27, 2021
1802 5.00.8634	May 1, 2018	No earlier than May 1, 2020
1606 5.00.8412	November 18, 2016	May 1, 2019

TIP

The EIC is supported for at least two years from the date of release. For more information on release dates, see Support for Configuration Manager current branch versions.

Plan to update the extended interoperability client on devices that you manage with the current branch before support for the client expires. To do so, download a new version of the client from Microsoft, and then deploy that updated client software to your devices that use the current extended interoperability client.

How to use the EIC

1. Add these devices to a collection, and exclude that collection from automatic client upgrades. For more information, see How to exclude clients from upgrade.

2. Obtain a supported version of the EIC from the `\SMSSETUP\Client` folder of the Configuration Manager update installation media. Make sure that you copy the entire contents of the folder.

   > **TIP**
   > To find Configuration Manager media in the Volume Licensing Service Center (VLSC), go to the **Downloads and Keys** tab, search for `System Center Config`, and then select **System Center Config Mgr (current branch)**.

3. Manually install the EIC on those devices. For more information, see Manually install the client.

   > **IMPORTANT**
   > When upgrading version 1606 clients to version 1802, use the CCMSETUP option **/AlwaysExcludeUpgrade:True**. Otherwise the client may receive policy from the management point to automatically upgrade before the exclusion policy.

Limitations

- Updates for the extended interoperability client software aren't available by using in-console updates. For more information on how to update the EIC, see How to upgrade an excluded client.
- The EIC only supports the following features:
  - Software updates
  - Hardware and software inventory
  - Packages and programs

Next steps

How to exclude clients from upgrade

To make sure that clients are installed correctly on the devices you want, see How to monitor clients.

Licensing and branches for System Center Configuration Manager

6/5/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch), (Long-Term Servicing Branch)

Use this article to learn about the licensing requirements for the installation options available with System Center Configuration Manager. These installation options include the following branches:

- Current branch
- Long-term servicing branch (LTSB)
- Evaluation installation of the current branch
- Technical preview branch

Licensing overview

Customers with active Software Assurance (SA) on System Center Configuration Manager licenses or with equivalent subscription rights as of October 1, 2016 have rights to use the October 2016 version 1606 release of System Center Configuration Manager. Customers with rights to System Center Configuration Manager on or after October 1, 2016 will find two licensed options upon installation: Current Branch and Long-Term Servicing Branch (LTSB).

For the complete terms and conditions for the products you purchase through Microsoft Volume Licensing programs, see Licensing Terms and Documentation.

Licensed branches

This article references the Software Assurance agreement or equivalent subscription rights. This Microsoft licensing agreement grants rights to install and use Configuration Manager.

Current branch

The current branch requires an active Software Assurance agreement or equivalent rights to Configuration Manager. For more information, see Software Assurance and the Current Branch.

This branch is supported for use in production environments that want to receive regular quality and feature updates from Microsoft. It provides access to use all features and improvements.

Beginning with the 1710 release, each update version remains in support for 18 months from its general availability release date. For more information, see Support for System Center Configuration Manager current branch versions.

Long-term servicing branch (LTSB)

The LTSB requires a current Software Assurance agreement with Microsoft as of October 1, 2016. For more information, see Software Assurance and the LTSB.

This branch is supported for use in production environments. It's intended for use by customers that have let their Software Assurance (SA) or equivalent subscriptions rights to Configuration Manager expire after October 1, 2016. This branch is limited when compared to the Current Branch.

Critical security updates for Configuration Manager are made available to this branch but no new features are made available.

Evaluation installation of the current branch

The evaluation version doesn't require a Software Assurance agreement with Microsoft. Evaluation installs are always the current branch, and you can use them for 180 days.

You can upgrade the evaluation installation to a full installation of the current branch. You can't upgrade an evaluation installation to the long-term servicing branch.

Technical preview branch

The technical preview branch is also available. This branch is a limited build of Configuration Manager that lets you try out new features. You install the technical preview using different media than the licensed versions. For more information, see Technical Preview.

Software Assurance agreements

The status of Software Assurance on your System Center Configuration Manager licenses, or equivalent subscription rights, on or after October 1, 2016, determines the branch you can install and use.

Software Assurance and the current branch

Rights to use Configuration Manager current branch can be provided by:

- **System Center:** Customers with active SA on System Center Standard or Datacenter licenses can install and use the current branch option of Configuration Manager.
- **System Center Configuration Manager:** Customers with active SA on System Center Configuration Manager licenses, or with equivalent subscription rights, can install and use the current branch option of Configuration Manager.

If you have active SA on System Center Configuration Manager licenses or equivalent subscription rights on or after October 1, 2016:

- You can install and use the current branch.
- If you allow SA or subscription to lapse, you must uninstall the current branch.

Software Assurance and the LTSB

If you have an active SA on System Center Configuration Manager licenses or equivalent subscription rights on or after October 1, 2016:

- You can install and use the LTSB. Customers who have perpetual rights to System Center Configuration Manager, or who allow their SA or subscription to lapse, can install the version of Configuration Manager LTSB that's current at the time of lapse.

LTSB is based on current branch version 1606, and has the following limitations:

- There's no support to convert a current branch to the LTSB. If you currently have a current branch site, you must install the LTSB as a new site.
- LTSB doesn't support all the capabilities of the current branch. For more information, see Introduction to the long-term servicing branch. These limitations include a limited feature set, limited upgrade options, and a separate product support lifecycle.

Software Assurance expiration date

Beginning with the October 2016 release of the version 1606 baseline media for Configuration Manager, you can specify the expiration date of your Software Assurance agreement. The **Software Assurance expiration date** is an optional value as a convenient reminder. Add it when you run Configuration Manager setup or later from within the Configuration Manager console.

> **NOTE**
>
> Microsoft doesn't validate the expiration date you specify, and doesn't use this date for license validation. Use it as a reminder of your expiration date. This value is useful when Configuration Manager periodically checks for new software updates offered online. Your Software Assurance license status should be current to be eligible to use these additional updates.

To specify the Software Assurance expiration date

- When you run Setup from the Configuration Manager media, specify the value on the **Product Key** page of the Setup wizard.
- In the Configuration Manager console, in **Hierarchy Settings**, specify the value on the **Licensing** tab.

Licensing resources

To learn more about product licensing details, use the following resources.

Microsoft Volume Licensing Service Center (VLSC)

- Overview of VLSC
- Microsoft Volume Licensing Product Terms
- Volume license customers can get a summary of their licenses from the Volume License Service Center. Go to the **Licenses** menu, and select **Licenses Summary**.

VLSC videos

- For training videos on how VLSC works, go to Microsoft Volume Licensing Service Center training and resources and select **How-to videos**.
- Where to look up your active Software Assurance agreement (starting at 43 seconds)
- How to get permissions for VLSC. You can delegate VLSC read and write permissions to other people in your organization.

Use cloud services with Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager supports several cloud-based options. These can supplement your on-premises infrastructure, and can help solve business problems like:

- How to manage BYOD (by using Intune for mobile device management).
- How to provide content resources to isolated clients or resources on the intranet, outside your corporate firewall (by using cloud-based distribution points).
- How to scale out infrastructure when physical hardware isn't available, or isn't logically placed to support your needs (by using Microsoft Azure virtual machines).

Although provisioning cloud resources is not something you must do before you deploy Configuration Manager, it can be beneficial to understand these options before progressing too far in a hierarchy design plan. The use of cloud resources might save you money and time, while solving business problems that on-premises infrastructure can't.

Cloud-based resources you can use with Configuration Manager

Because each option has different requirements, investigate each in greater depth to understand the unique prerequisites, limitations, and potential for additional costs based on use.

- For information about cloud-based distribution points, see Install cloud-based distribution points.
- For more information about Azure, see Azure in the MSDN Library.

Azure virtual machines (for cloud-based infrastructure)

Configuration Manager supports using computers that run in virtual machines in Azure, just as it does when run on-premises within your physical corporate network. You can use Azure virtual machines in the following scenarios:

- **Scenario 1:** You can run Configuration Manager in a virtual machine and use it to manage clients installed in other virtual machines.
- **Scenario 2:** You can run Configuration Manager in a virtual machine and use it to manage clients that are not running in Azure.
- **Scenario 3:** You can run different Configuration Manager site system roles in virtual machines, while running other roles in your physical corporate network (with appropriate network connectivity for communications).

The same requirements for networks, operating systems, and hardware requirements that apply to installing the Configuration Manager on your physical corporate network also apply to the installation of Configuration Manager in Azure.

An Azure subscription is required to use Azure virtual machines. You incur charges based on the number of virtual machines you use, their configuration, and use of cloud-based resources.

Additionally, Configuration Manager sites and clients that run in Azure virtual machines are subject to the same license requirements as on-premises installations.

Azure services (for cloud-based distribution points)

You can use an Azure service to host a Configuration Manager distribution point, which is called a called cloud-based distribution point. You can use a cloud-based distribution point with System Center Configuration Manager alongside on-premises distribution points, and distribution points deployed in Azure virtual machines.

This is different than using an Azure virtual machine, on which you deploy a site system role. Cloud-based distribution points:

- Run as a service in Azure, not on a virtual machine.
- Automatically scale to meet increased content requests from clients.
- Support clients on the Internet and the intranet.

An Azure subscription is required to use Azure to host distribution points. You incur charges based on the amount of data that transfers to and from the service.

Additional Configuration Manager capabilities

Some Configuration Manager capabilities can connect to cloud-based services, like:

- Windows Server Update Services (WSUS).
- The Configuration Manager service cloud, to download updates for Configuration Manager.

These additional capabilities do not require you to have an Azure subscription. You don't have to set up specific connections, certificates, or services in the cloud. Instead, they are automatically managed by Configuration Manager for you. All you need to do is ensure applicable site systems and devices can access the Internet-based URLs.

Security for cloud-based services

Configuration Manager uses certificates to provision and access your content in Azure, and to manage the services that you use. Configuration Manager encrypts the data that you store in Azure, but does not introduce additional security or data controls beyond those that Azure provides.

For more information, see the details for the different cloud-based resource scenarios. You can also view the following topics for Azure security:

- Azure: Understanding Security Account Management in Azure
- Azure Security Overview
- Get Past the Security Crossroads in Your Cloud Migration
- Data Security in Azure Part 1 of 2

Configuration Manager on Azure - Frequently Asked Questions

9/11/2019 • 10 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The following questions and answers can help you understand when to use and how to configure Configuration Manager on Microsoft Azure.

General Questions

My company is trying to move as many physical servers as possible to Microsoft Azure, can I move Configuration Manager servers to Azure?

Certainly, this is a supported scenario. See Support for Virtualization Environments for System Center Configuration Manager.

Great! My environment requires multiple sites. Should all child primary sites be in Azure with the central administration site or on-premises? What about secondary sites?

Site-to-site communications (file-based and database replication) benefits from the proximity of being hosted in Azure. However, all client related traffic would be remote from site servers and site systems. If you use a fast and reliable network connection between Azure and your intranet with an unlimited data plan, hosting all your infrastructure in Azure is an option.

However, if you use a metered data plan and available bandwidth or cost is a concern, or the network connection between Azure and your intranet is not fast or can be unreliable, then consider placing specific sites (and site systems) on-premises and then use the bandwidth controls built into Configuration Manager.

Is having Configuration Manager in Azure a SaaS scenario (Software as a Service)?

No, it is an IaaS (Infrastructure as a Service) because you host your Configuration Manager infrastructure servers in Azure virtual machines.

What areas should I pay attention to when considering a move of my Configuration Manager infrastructure to Azure?

Great question, here are the areas that are most important when making this decision, each is explored in a separate section of this topic:

1. Networking
2. Availability
3. Performance
4. Cost
5. User Experience

Networking

What about networking requirements, should I use ExpressRoute or an Azure VPN Gateway?

Networking is a very important decision. Network speeds and latency can affect functionality between the site server and remote site systems and any client communication to the site systems. Our recommendation is to use ExpressRoute. But there is no Configuration Manager limitation to stop you from using Azure VPN Gateway. You should carefully review your requirements (performance, patching, software distribution, operation system deployment) from this infrastructure and then make your decision. Some things to consider for each solution

include:

- **ExpressRoute** (recommended)
  - Natural extension to your datacenter (can tie together multiple datacenters)
  - Private connections between Azure datacenters and your infrastructure
  - Doesn't go over the public internet
  - Offers reliability, fast speeds, lower latency, high security
  - Offers up to 10gbps speeds and Unlimited Data plan options
- **VPN Gateway**
  - Site-to-site/point-to-site VPNs
  - Traffic goes over the public internet
  - Uses Internet Protocol Security (IPsec) and Internet Key Exchange (IKE)

ExpressRoute has many different options like unlimited vs. metered, different speed options, and premium add-on. Which should I choose?

The options you select depend on the scenario you are implementing and how much data you plan to distribute. The transfer of Configuration Manager data can be controlled between site servers and distribution points, but site server-to-site server communication can't be controlled. When you use a metered data plan, placing specific sites (and site systems) on-premises and using Configuration Manager's built-in bandwidth controls can help control the cost of using Azure.

What about installation requirements like Active Directory domains? Do I still need to join my site servers to an Active Directory domain?

Yes. When you move to Azure, the supported configurations remain the same, including Active Directory requirements for installing Configuration Manager.

I understand the need to join my site servers to an Active Directory domain, but can I use Azure Active Directory?

No, Azure Active Directory is not supported at this time. Your site servers still must be members of a Windows Active Directory domain.

Availability

One of the reasons I am moving infrastructure to Azure is the promise of high availability. Can I take advantage of high availability options like Azure VM Availability sets for VMs that I will use for Configuration Manager?

Yes! Azure VM Availability sets can be used for redundant site system roles like distribution points or management points.

You can also use them for the Configuration Manager site servers. For example, central administration sites and primary sites can all be in the same availability set which can help you ensure that they are not rebooted at the same time.

How can I make my database highly available? Can I use Azure SQL Database? Or do I have to use Microsoft SQL Server in a VM?

You need to use Microsoft SQL Server in a VM. Configuration Manager does not support Azure SQL Server at this time. But you can use functionalities like AlwaysOn Availability Groups for your SQL server. AlwaysOn Availability Groups are recommended and are officially supported starting with version 1602 of Configuration Manager.

Can I use Azure load balancers with site system roles like management points or software update points?

While Configuration Manager is not tested with Azure load balancers, if the functionality is transparent to the application, it should not have any adverse effects on normal operations.

Performance

What factors affect performance in this scenario?

Azure VM size and type, Azure VM disks (premium storage is recommended, especially for SQL Server), networking latency, and speed are the most important areas.

So, tell me more about Azure virtual machines; what size VMs should I use?

In general, your compute power (CPU and Memory) need to meet the recommended hardware for System Center Configuration Manager. But there are some differences between regular computer hardware and Azure VMs, especially when it comes to the disks these VMs use. What size VMs you use depends on the size of your environment but here are some recommendations:

- For production deployments of any significant size we recommend "**S**" class Azure VMs. This is because they can leverage Premium Storage disks. Non "S" class VMs use blob storage and in general will not meet the performance requirements necessary for an acceptable production experience.
- Multiple Premium Storage disks should be used for higher scale, and striped in the Windows Disk Management console for maximum IOPS.
- We recommend using better or multiple premium disks during your initial site deployment (like P30 instead of P20, and 2xP30 in a striped volume instead of 1xP30). Then, if your site later needs to ramp up in VM size due to additional load, you can take advantage of the additional CPU and memory that a larger VM size provides. You will also have disks already in place that can take advantage of the additional IOPS throughput that the larger VM size allows.

The following tables list the initial suggested disk counts to utilize at primary and central administration sites for various size installations:

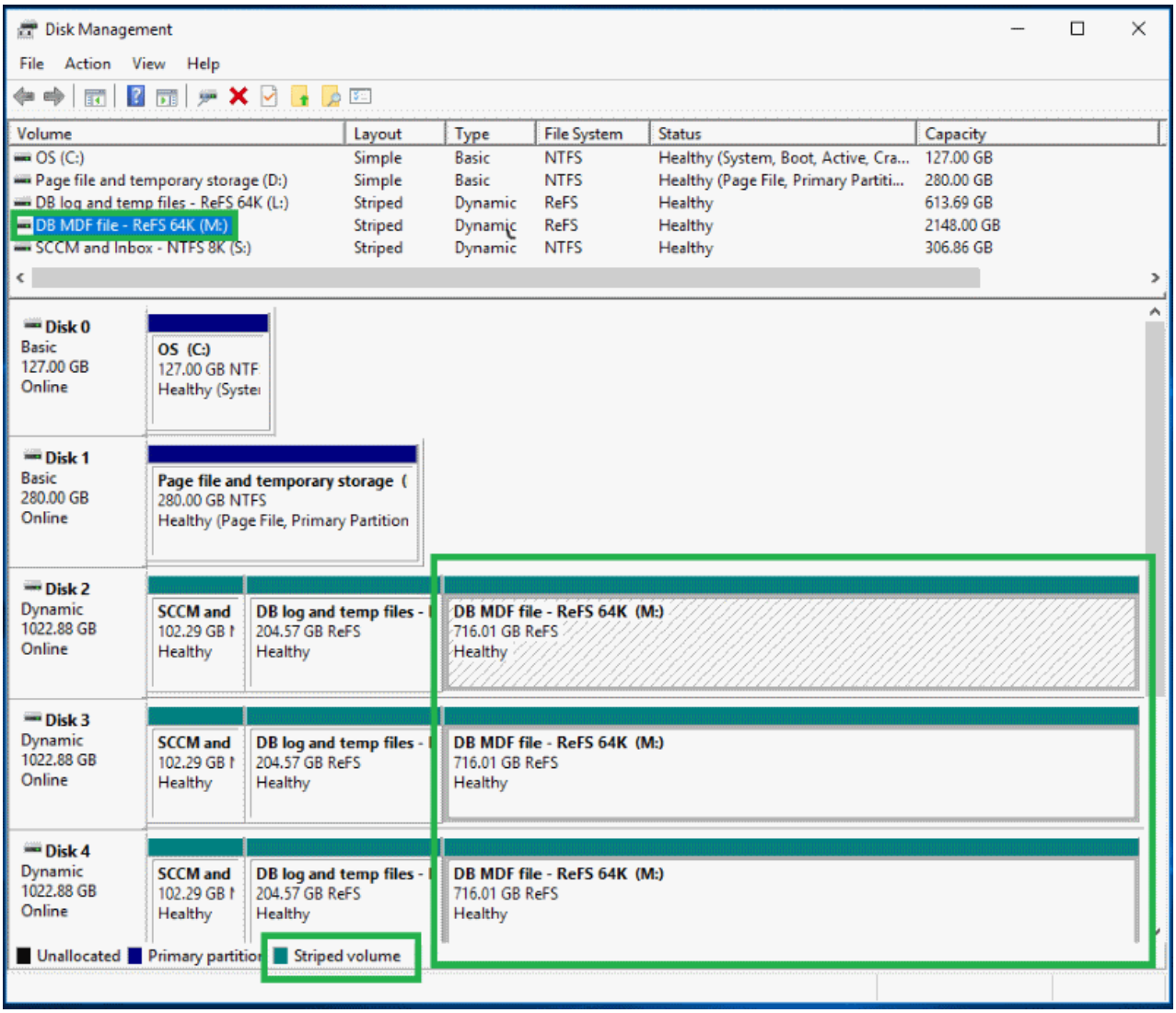
Co-located site database - Primary or central administration site with the site database on the site server:

DESKTOP CLIENTS	RECOMMENDED VM SIZE	RECOMMENDED DISKS
Up to 25k	DS4_V2	2xP30 (striped)
25k to 50k	DS13_V2	2xP30 (striped)
50k to 100k	DS14_V2	3xP30 (striped)

Remote site database - Primary or central administration site with the site database on a remote server:

DESKTOP CLIENTS	RECOMMENDED VM SIZE	RECOMMENDED DISKS
Up to 25k	Site server: F4S Database server: DS12_V2	Site server: 1xP30 Database server: 2xP30 (striped)
25k to 50k	Site server: F4S Database server: DS13_V2	Site server: 1xP30 Database server: 2xP30 (striped)
50k to 100k	Site server: F8S Database server: DS14_V2	Site server: 2xP30 (striped) Database server: 3xP30 (striped)

The following shows an example configuration for 50k to 100k clients on DS14_V2 with 3xP30 disks in a striped volume with separate logical volumes for the Configuration Manager install and database files:



User Experience

You mention that user experience is one of the main areas of importance, why is that?

The decisions you make for networking, availability, performance, and where you place your Configuration Manager site servers can affect your users directly. We believe a move to Azure should be transparent to your users so that they don't experience a change in their day-to-day interactions with Configuration Manager.

Ok, I get it. I plan to install a single stand-alone primary site on an Azure virtual machine and I want to make sure my costs are low. Should I place (remote) site systems (like management points, distribution points, and software update points) on Azure virtual machines as well or on-premises?

Except for communication from the site server to a distribution point, these server-to-server communications in a site can occur at any time and do not use mechanisms to control the use of network bandwidth. Because you cannot control the communication between site systems, any costs associated with these communications should be considered.

Network speeds and latency are other factors to consider as well. Slow or unreliable networks could impact functionality between the site server and remote site systems as well any client communication to the site systems. The number of managed clients that use a given site system as well as the features you actively use should also be considered. In general, you can leverage the normal guidance as it relates to WAN links and site systems as a starting point. Ideally, the network throughput that you select and receive between Azure and your intranet will be consistent with a WAN that is well-connected with a fast network.

What about content distribution and content management? Should standard distribution points be in Azure or on-premises, and should I use BranchCache or pull-distribution points on-premises? Or should I make exclusive use of Cloud Distribution Points?

The approach for content management is much the same as for site servers and site systems.

- If you use a fast and reliable network connection between Azure and your intranet with an unlimited data plan, hosting standard distribution points in Azure could be an option.
- If you use a metered data plan and bandwidth cost is a concern or the network connection between Azure and your intranet is not fast or can be unreliable, then you might consider other approaches. These include locating standard or pull distribution points on-premises as well as using BranchCache. The use of cloud-based distribution points is also an option but there are some limits on the content types supported (for example, no support for software updates packages).

> **NOTE**
> If PXE or multicast support is required, you must use on-premises distribution points (standard or pull) to respond to boot requests.

While I am OK with the limitations of cloud-based distribution points, I don't want to put my management point into a DMZ even though that is needed to support my internet-based clients. Do I have any other options?

Yes! With the Configuration Manager version 1610, we introduced the Cloud Management Gateway as a pre-release feature. (This feature first appeared in the Technical Preview version 1606 as the Cloud Proxy Service).

The **Cloud Management Gateway** provides a simple way to manage Configuration Manager clients on the internet. The service, which is deployed to Microsoft Azure and requires an Azure subscription, connects to your on-premises Configuration Manager infrastructure using a new role called the cloud management gateway connector point. After it's deployed and configured, clients can access on-premises Configuration Manager site system roles regardless of whether they're connected to the internal private network or on the internet.

You can start using the cloud management gateway in your environment and give us feedback to make this better. For information about pre-release features, see Use pre-release features from updates.

I also heard that you have another new feature called Peer Cache introduced as a pre-release feature in version 1610. Is that different than BranchCache? Which one should I choose?

Yes, totally different. Peer Cache is a 100% native Configuration Manager technology where BranchCache is a feature of Windows. Both can be useful for you; BranchCache uses a broadcast to find the required content whereas Peer Cache uses Configuration Managers regular distribution workflow and boundary group settings.

You can configure any client to be a Peer Cache source. Then, when management points provide clients information about content source locations, they provide details about both the distribution points and any Peer Cache sources that have the content that client requires.

Cost

OK tell me a bit about the cost. Will this be a cost-effective solution for me?

Hard to say since every environment is different. The best thing to do is to cost your environment using Microsoft Azure pricing calculator: https://azure.microsoft.com/pricing/calculator/

Additional Resources

Fundamentals: https://azure.microsoft.com/documentation/articles/fundamentals-introduction-to-azure/

Azure VM Machine Types:

- Azure Machine sizes: https://azure.microsoft.com/documentation/articles/virtual-machines-size-specs/
- VM Pricing: https://azure.microsoft.com/pricing/details/virtual-machines/
- Storage Pricing: https://azure.microsoft.com/pricing/details/storage/

Disk Performance Considerations:

- Premium Disk intro: https://azure.microsoft.com/blog/2014/12/11/introducing-premium-storage-high-performance-storage-for-azure-virtual-machine-workloads/
- Deeper Premium Disk info: https://azure.microsoft.com/documentation/articles/storage-premium-storage-preview-portal/
- Handy collection of charts for max Sizes and Perf targets for Storage: https://azure.microsoft.com/documentation/articles/storage-scalability-targets/
- Another Intro + some cool uber-geek data on how Premium Storage works behind the covers: https://azure.microsoft.com/blog/2015/04/16/azure-premium-storage-now-generally-available-2/

Availability:

- Azure IaaS Uptime SLA's: https://azure.microsoft.com/support/legal/sla/virtual-machines/v1_0/
- Availability Sets Explained: https://azure.microsoft.com/documentation/articles/virtual-machines-manage-availability/

Connectivity:

- Express route vs. Azure VPN: https://azure.microsoft.com/blog/2014/06/10/expressroute-or-virtual-network-vpn-whats-right-for-me/
- Express Route Pricing: https://azure.microsoft.com/pricing/details/expressroute/
- More about Express Route: https://azure.microsoft.com/documentation/articles/expressroute-introduction/

Frequently asked questions for Configuration Manager branches and licensing

9/6/2019 • 7 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch), System Center Configuration Manager (Long-Term Servicing Branch)

This FAQ addresses common licensing questions about Configuration Manager current branch and the long-term servicing branch (LTSB) versions, available through Microsoft Volume Licensing programs. This article is for informational purposes. It doesn't supersede or replace any documentation covering System Center Configuration Manager licensing. For more information, see the product licensing for System Center 2016 and the Product Terms. The Product Terms describe the use terms for all Microsoft products in Volume Licensing.

For more information about Configuration Manager features, see the product page.

What's current branch?

The current branch is the production-ready build of Configuration Manager that provides an active servicing model. This servicing model is like the experience with Windows 10. This approach supports customers who are moving at a "cloud cadence" and wish to innovate more quickly. With the current branch servicing model, you continue to receive new features and functionality. For this reason, only customers with active Software Assurance on Configuration Manager licenses, or with equivalent subscription rights, may install and use the current branch of Configuration Manager.

What's the long-term servicing branch (LTSB)?

The LTSB is a production-ready build of Configuration Manager. It's intended for customers who allow Software Assurance or equivalent subscription rights to expire. When compared to the current branch, the LTSB has reduced functionality. Customers who allow Software Assurance or equivalent subscription rights to expire must uninstall the current branch of Configuration Manager. Customers who have perpetual license rights to Configuration Manager may then install and use the LTSB build of the Configuration Manager version that's current at the time of expiration.

I've seen *SA* and *L&SA* used in licensing content. What do these acronyms mean in regard to Configuration Manager?

Both **Software Assurance** (SA) and **License and Software Assurance** (L&SA) are license options that grant rights to use Configuration Manager. SA is an option for a customer that's renewing SA coverage from a prior agreement. L&SA is an option for a customer buying a new license and SA coverage.

- **Software Assurance (SA)**: Customers must have active SA on Configuration Manager licenses, or equivalent subscription rights, in order to install and use the current branch option of Configuration Manager.
    - While SA is optional for some Microsoft products, the only way to get rights to use Configuration Manager current branch is with SA *or equivalent subscription rights*. For more information, see the Software Assurance FAQ.
- **Microsoft License and Software Assurance (L&SA)**: Customers buying new licenses for Configuration Manager must acquire L&SA (the license and SA coverage).
    - The SA grants rights to use the current branch.
    - If your SA expires, and you still have a license for Configuration Manager, you can no longer use the current branch. For more information, see the FAQ If my SA expires and I had L&SA, what do I get?

For more information about license offerings, see Ways to buy and Licensing Product Terms.

I read the term "equivalent subscription", what programs does that refer to?

Equivalent subscriptions refer to programs like Enterprise Mobility + Security (EMS) or Microsoft 365 Enterprise. There can be others, but these programs are the most common. The Microsoft Volume Licensing Product Terms refers to these programs as Management License Equivalent Licenses.

I have Enterprise Mobility + Security and it expired, what must I do now?

EMS grants rights to use Configuration Manager current branch and long-term service branch. When these rights expire, you no longer have rights to use either branch and must uninstall.

If my SA expires, and I had L&SA, what do I get?

If your SA expired after October 1, 2016, depending on what program you acquired L&SA under, you could retain a perpetual license to use the LTSB. If you currently use the current branch, you must uninstall it, and then install the LTSB. There's no support to migrate or convert to the LTSB from the current branch.

If your SA expired before October 1, 2016, and you retained a perpetual license to Configuration Manager, then your only option for ongoing use is to install and use System Center 2012 R2 Configuration Manager and its available service packs. You're required to uninstall the current branch when your SA expires, and reinstall that earlier version of the product. There's no support to migrate to or downgrade from Configuration Manager current branch to prior versions of Configuration Manager.

If you use System Center Endpoint Protection, and your SA expires, you must uninstall it. System Center Endpoint Protection offers no *L (License)* rights, and no perpetual rights.

Do I "own" the current branch?

No. You're licensed to use the current branch while you have active SA. For example, via *L&SA*, when *SA* expires, you then have only *L (License)* rights, which don't include rights to use the current branch. If your L provides perpetual rights, you can use the Configuration Manager LTSB in place of the current branch. If your SA expired prior to October 1, 2016, you can also use System Center 2012 R2 Configuration Manager.

Can I purchase Configuration Manager standalone without SA?

No. The only way to get rights to use Configuration Manager is to acquire a license with SA or through an equivalent subscription. There are developer programs like MSDN where Configuration Manager is offered for development and test purposes, but not production usage.

I see updates for Configuration Manager offered from within my console, like version 1810. Do I have rights to install it?

If you have active *SA*, you do have rights. If you don't have active SA, uninstall the current branch, and then install the LTSB of Configuration Manager. The LTSB doesn't receive updates for incremental versions of Configuration Manager, but does receive security updates based on the Support Lifecycle.

I have purchased EMS or Microsoft 365 through a Cloud Solution Provider (CSP), do I have rights to use Configuration Manager?

Yes, you have rights to use Configuration Manager to manage clients covered by the EMS license. First download and install the evaluation software. Then contact Microsoft Support to obtain the license key. When you talk with Microsoft Support, ask them to reference the internal article ID 4033838.

Is my subscription end-date the same as an SA expiration date?

If *SA* or your subscription is active, you have use rights for Configuration Manager current branch. An active subscription is equivalent of having active *SA*, but no perpetual *"L" (license)*. Once your subscription is over, uninstall the current branch. At this time, you don't have rights to use the LTSB.

What are the use rights associated with the SQL technology provided with Configuration Manager?

All of the System Center products include SQL Server technology. Microsoft's licensing terms for these products

allow customer use of SQL Server technology only to support System Center components. SQL Server client access licenses are not required for that use.

Approved use rights for the SQL capabilities with Configuration Manager include:

- Site database role
- Windows Server Update Services (WSUS) for software update point role
- SQL Server Reporting Services (SSRS) for reporting point role
- Data warehouse service point role
- Database replicas for management point roles
- SQL Server Always On

The SQL Server license that's included with Configuration Manager supports each instance of SQL Server that you install to host a database for Configuration Manager. However, only databases for Configuration Manager in the preceding list can run on that SQL Server when you use this license. If a database for any additional Microsoft or third-party product shares the SQL Server, you must have a separate license for that SQL Server instance.

Does on-premises mobile device management (MDM) require an Intune subscription?

In versions 1806 and earlier, to start using on-premises MDM, you need a Microsoft Intune subscription. The subscription is only required to track licensing of the devices and isn't used to manage or store management information for the devices. All management data is stored in your organization using the on-premises Configuration Manager infrastructure.

Starting in version 1810, an Intune connection is no longer required for new on-premises MDM deployments. Your organization still requires Intune licenses to use this feature. You can't currently remove the Intune connection from existing on-premises MDM deployments. For more information, see the Intune support blog post.

System Center Configuration Manager site sizing and performance FAQ

5/17/2019 • 14 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This document addresses frequently asked questions about Configuration Manager site sizing guidance and common performance issues.

Machine and disk configuration FAQs and examples

How should I format the disks on my site server and SQL Server?

Separate the Configuration Manager inboxes and SQL files on at least two different volumes. This separation lets you optimize cluster allocation sizes for the different kinds of I/O they perform.

For the volume hosting your sites server inboxes, use NTFS with 4K or 8K allocation units. ReFS writes 64k even for small files. Configuration Manager has many small files, so ReFS can produce unnecessary disk overhead.

For disks containing SQL database files, use either NTFS or ReFS formatting, with 64K allocation units.

How and where should I lay out my SQL database files?

Modern arrays of solid-state drives (SSD) and Azure Premium Storage can provide high IOPS on a single volume, with few disks. You typically add more drives to an array for additional storage, not additional throughput. If you're using physical spindle-based disks, you may need more IOPS than you can generate on a single volume. You should allocate 60% of the total recommended IOPS and disk space for the *.mdf* file, 20% for the *.ldf* file, and 20% for the log and data temp files. The *.ldf* and temp files can all reside on a single volume with 40% (20% + 20%) of your allocated IOPS.

By default, SQL creates one temp data file. You should create more, to avoid SQL locks and waiting for access to a single file. Community opinions vary on the best number of temp data files to create, from four to eight. Testing reveals little difference between four to eight, so you can create four *equally sized* temp data files. Your tempdb data files should be up to 20-25% the size of your full database.

Are there any other recommendations for disk setup?

When configurable, set RAID controller memory to 70% allocation for write operations and 30% for read operations. In general, use a RAID 10 array configuration for the site database. RAID 1 is also acceptable for small-scale sites with low I/O requirements, or if you use fast SSDs. With larger disk arrays, configure spare disks to automatically replace failing disks.

Example: Physical machine with physical disks

Sizing guidelines for a colocated site server and SQL server with **100,000** clients are 1200 IOPS for site server inboxes and 5000 IOPS for SQL Server files.

Your resulting disk configuration might look like:

DRIVES[1]	RAID	FORMAT	VOLUME CONTENTS	MINIMUM IOPS NEEDED	APPROX. IOPS SUPPLIED[2]
2x10k	1	-	Windows		-

DRIVES	RAID	FORMAT	VOLUME CONTENTS	MINIMUM IOPS NEEDED	APPROX. IOPS SUPPLIED
6x15k	10	NTFS 8k	ConfigMgr inboxes	1700	1751
12x15k	10	64k ReFS	SQL .mdf	60%*5000 = 3000	3476
8x15k	10	64k ReFS	SQL .ldf, temp files	40%*5000 = 2000	2322

1. Doesn't include recommended spare disks.
2. This value is from Example disk configurations.

I use Hyper-V on Windows Server. How should I configure the disks for my Configuration Manager VMs for best performance?

Hyper-V delivers similar performance to a physical server, if hardware resources (CPU cores and pass-through storage) are 100% dedicated to the virtual machine (VM). Using fixed-size *.vhd* or *.vhdx* disk files causes a minimal 1-5% I/O performance impact. Using dynamically expanding *.vhd* or *.vhdx* disk files causes up to 25% I/O performance impact for the Configuration Manager workload. If you need dynamically expanding disks, compensate by adding an additional 25% IOPS performance to the array.

When running your Configuration Manager site server or SQL inside a VM, isolate the Hyper-V host OS drives from the VM OS and data drives.

For more information about optimizing VMs, see Performance Tuning Hyper-V Servers.

Example: Hyper-V VM-based site server

Sizing guidelines for a colocated site server and SQL server with **150,000** clients are 1800 IOPS for site server inboxes and 7400 IOPS for SQL Server files.

Your resulting disk configuration might look like:

DRIVES[1]	RAID	FORMAT[2]	VOLUME CONTENTS	MINIMUM IOPS NEEDED	APPROX. IOPS SUPPLIED[3]
2x10k	1	-	Hyper-V host OS	-	-
2x10k	1	-	(VM) site server OS	-	-
2xSSD SAS	1	NTFS 8k	(VM) ConfigMgr inboxes	1800	7539
4xSSD SAS	10	64k ReFS	(VM) Host SQL (all files)	7400	14346

1. Doesn't include recommended spare disks.
2. Fixed-size, pass-through *.vhdx* for the VM drive dedicated to the underlying volume.
3. This value is from Example disk configurations.

Are there any suggestions for Configuration Manager environments in Microsoft Azure?

Start by reading the Configuration Manager on Azure frequently asked questions.

Azure infrastructure as a service (IaaS) VMs that leverage Premium Storage-based disks can have high IOPS. On

these VMs, configure additional disks for anticipated disk space needs, rather than for additional IOPS.

Azure storage is inherently redundant and doesn't require multiple disks for availability. You can stripe disks in Disk Manager or Storage Spaces to provide additional space and performance.

For more information and recommendations on how to maximize Premium Storage performance and run SQL servers in Azure IaaS VMs, see:

- Optimize application performance
- Disks guidance

Example: Azure-based site server

Sizing guidelines for a colocated site server and SQL server with **50,000** clients are eight cores, 32 GB, and 1200 IOPS for site server inboxes, and 2800 IOPS for SQL Server files.

Your resulting Azure machine might be a DS13v2 (eight cores, 56 GB) with the following disk configuration:

DRIVES	FORMAT	CONTAINS	MINIMUM IOPS NEEDED	APPROX. IOPS SUPPLIED[1]
<standard>	-	Site server OS	-	-
1xP20 (512 GB)	NTFS 8k	ConfigMgr inboxes	1200	2334
1xP30 (1024 GB)	64k ReFS	SQL (all files[2])	2800	3112

1. This value is from Example disk configurations.
2. Azure guidance allows for placing the TempDB on the local, SSD-based *D:* drive, given it won't exceed available space and allows for additional disk I/O distribution.

Example: Azure-based site server (for instant performance increase)

Azure disk throughput is limited by the size of the VM. The configuration in the preceding Azure example may limit future expansion or additional performance. If you add additional disks during initial deployment of your Azure VM, you can upsize your Azure VM for increased processing power in the future, with minimal upfront investment. It's much simpler to plan ahead to increase site performance as requirements change, instead of later needing to do a more complicated migration.

Change the disks in the preceding Azure example to see how the IOPS change.

DS13v2

DRIVES[1]	FORMAT	CONTAINS	MINIMUM IOPS NEEDED	APPROX. IOPS SUPPLIED[2]
<standard>	-	Site server OS	-	-
2xP20 (1024 GB)	NTFS 8k	ConfigMgr inboxes	1200	3984
2xP30 (2048 GB)	64k ReFS	SQL (all files[3])	2800	3984

1. Disks are striped using Storage Spaces.
2. This value is from Example disk configurations. VM size limits performance.
3. Azure guidance allows for placing the TempDB on the local, SSD-based *D:* drive, given it won't exceed available space and allows for additional disk I/O distribution.

If you need more performance in future, you can upsize your VM to a DS14v2, which will double CPU and memory. The additional disk bandwidth allowed by that VM size will also instantly boost the available disk IOPS on your previously configured disks.

DS14v2

DRIVES[1]	RAID	FORMAT	CONTAINS	MINIMUM IOPS NEEDED	APPROX. IOPS SUPPLIED[2]
<standard>	-	Site server OS	-	-	
2xP20 (1024 GB)	NTFS 8k	ConfigMgr inboxes	1200	4639	
2xP30 (2048 GB)	64k ReFS	SQL (all files[3])	2800	6182	

1. Disks are striped using Storage Spaces.
2. This value is from Example disk configurations. VM size limits performance.
3. Azure guidance allows for placing the TempDB on the local, SSD-based *D:* drive, given it won't exceed available space and allows for additional disk I/O distribution.

Other common SQL Server-related performance questions

Is it better to run with SQL colocated with the site server, or run it on a remote server?

Both can perform adequately, assuming the single server is appropriately sized, or network connectivity is sufficient between the two servers.

Remote SQL requires the upfront and operational cost of an additional server, but is typical among the majority of large-scale customers. Benefits of this configuration include:

- Increased site availability options, such as SQL Always On
- Ability to run heavy reporting with less overheard to site processing
- Simpler disaster recovery in some situations
- Easier security management
- Role separation for SQL management, such as with a separate DBA team

Colocated SQL requires a single server, and is typical for most small-scale customers. Benefits of this configuration include:

- Lower costs for machines, licenses, and maintenance
- Fewer points of failure in the site
- Better control for planning downtime

How much RAM should I allocate for SQL?

By default, SQL uses all available memory on your server, potentially starving the OS and other processes on the machine. To avoid potential performance issues, it's important to allocate memory to SQL explicitly. On site servers colocated with SQL servers, make sure the OS has enough RAM for file caching and other operations. Make sure there's enough RAM remaining for SMSExec and other Configuration Manager processes. When running SQL on a remote server, you can allocate the *majority* of the memory to SQL, but not all. Review the sizing guidelines for initial guidance.

SQL Server memory allocation should be rounded to whole GB. Also, as RAM increases to large amounts, you can let SQL have a higher percentage. For example, when 256 GB or more of RAM is available, you can configure SQL for up to 95%, as that still preserves plenty of memory for the OS. Monitoring the page file is a good way to ensure there is enough memory for the OS and any Configuration Manager processes.

Cores are cheap these days. Should I just add a bunch of them to my SQL server?

You may run into memory contention issues if there are more than 16 physical cores and not enough RAM on your SQL server. The Configuration Manager workload performs better when at least 3-4 GB of RAM per core is available for SQL. When adding cores to your SQL servers, be sure to increase RAM in proportional amounts.

Will SQL Always On impact my performance?

In general, SQL Always On has negligible effect on performance of the system when sufficient networking is available between the SQL replica servers. You can have rapid database log *.ldf* file growth in a busy SQL Always On environment. However, log file space is automatically released after a successful database backup. Add a SQL job for the Configuration Manager database to perform a backup, for example every 24 hours, and an *.ldf* backup every six hours. For more information about SQL Always On and Configuration Manager, including more about SQL backup strategies, see SQL Server Always On for a highly available site database.

Should I enable SQL compression on my database?

SQL compression isn't recommended for the Configuration Manager database. While there are no functional issues with enabling compression on a Configuration Manager database, test results don't show much size savings compared to the potential sizable performance impact to the system.

Should I enable SQL encryption on my database?

Any secrets in the Configuration Manager database are already stored securely, but adding SQL encryption can add yet another layer of security. There are no functional issues with enabling encryption on your database, but there can be up to a 25% performance degradation, depending on the tables you choose to encrypt and the version of SQL you're using. Therefore, encrypt with caution, especially in large-scale environments. Also remember to update your backup and recovery plans to ensure you can successfully recover the encrypted data.

What version of SQL should I run?

For supported versions of SQL, see Support for SQL Server versions. From a performance standpoint, all supported versions of SQL meet required performance criteria. However, SQL 2012 and SQL 2016 or newer tend to outperform SQL 2014 in some aspects of the Configuration Manager workload. Also, running SQL 2014 at SQL 2012 compatibility level (110) improves performance in general. At installation time, Configuration Manager databases running on SQL 2012 and SQL 2014 are set to compatibility level 110. SQL 2016 or newer is set to that SQL version's default compatibility level, such as 130 for SQL 2016. Upgrading SQL in place doesn't update compatibility levels until you install the next major Configuration Manager current branch version.

If you see unusual timeouts or slowness on certain SQL queries on SQL 2016 or later, such as when using RBAC in the Admin Console, try changing the SQL compatibility level on the Configuration Manager database to 110. Running at SQL compatibility level 110 on SQL 2014 and newer versions of SQL is fully supported. For more information, see SQL query times out or console slow on certain Configuration Manager database queries.

As of January 2018, you should *avoid* the following SQL versions, because of various known performance-related or other potential issues:

- SQL 2012 SP3 CU1 to CU5
- SQL 2014 SP1 CU6 to SP2 CU2
- SQL 2016 RTM to CU3, SP1 CU3 to CU5

Should I implement any additional SQL indexing tasks?

Yes, update indexes as often as once a week and statistics as often as once a day to improve SQL performance. Third-party scripts and additional information available from the Configuration Manager and SQL communities can help optimize these tasks.

In large sites, some SQL tables, such as CI_CurrentComplianceStatusDetails, HinvChangeLog, might be large, depending on your usage patterns. You may need to reduce or alter your maintenance approach for them one by one.

When should I use full SQL Server instead of SQL Express on my secondary sites?

SQL Express doesn't have any significant performance implications on secondary sites, and it's adequate for most customers. It's also easy to deploy and manage, and is the recommended configuration for nearly all customers at any size.

There's one situation where a full SQL Server installation might be needed. If you have a large number of distribution points and packages or sources in your environment, it's possible to exceed the 10-GB size limit of SQL Express. If the number of packages times the number of distribution points is more than 4,000,000, such as 2,000 DPs with 2,000 pieces of content, consider using full SQL Server at your secondary sites.

Should I change MaxDOP settings on my database?

Leaving your setting at 0 (use all available processors) is optimal for overall processing performance in most circumstances.

Many Configuration Manager administrators follow the guidance at Recommendations and guidelines for the "max degree of parallelism" configuration option in SQL Server. On most modern large hardware, this guidance leads to a suggested maximum setting of eight. However, if you run many smaller queries compared to your number of processors, it may help to set it to a higher number. Limiting yourself to eight isn't necessarily the best setting on larger sites when more cores are available.

On SQL servers with greater than eight cores, start with a setting of 0, and only make changes if you experience performance issues or excessive locking. If you need to change MaxDOP because you are encountering performance issues at 0, start with a new value at least greater than or equal to the minimum recommended number of cores for that site's SQL server sizing. Going lower than this value nearly always has negative performance implications. For example, a remote SQL server for a 100,000 client site needs at least 12 cores. If your SQL server has 16 cores, start testing your MaxDOP setting with a value of 12.

Other common performance-related questions

Which folders on the site server (or other roles) should I exclude for antivirus software?

Take care when disabling antivirus protection on any system. In high volume and secure environments, we recommend disabling *active monitoring* for optimum performance.

For more information about recommended antivirus exclusions, see Recommended antivirus exclusions for Configuration Manager 2012 and Current Branch Site Servers, Site Systems, and Clients.

What can I do to make WSUS perform better when it's used with Configuration Manager?

Changing a few key IIS settings, such as WsusPool Queue Length and WsusPool Private Memory limit, can improve WSUS performance, even on smaller installations. For more information, see Recommended hardware.

Also make sure you have the latest updates installed for the operating system running WSUS:

- Windows Server 2012: Any non "Security only" cumulative update released October 2017 or later. (KB4041690)
- Windows Server 2012 R2: Any non "Security only" cumulative update released August 2017 or later. (KB4039871)
- Window Server 2016: any non "Security only" cumulative update released August 2017 or later. (KB4039396)

What type of maintenance should I run on my WSUS servers?

See The complete guide to Microsoft WSUS and Configuration Manager SUP maintenance.

I want to set up basic performance monitoring for my site. What should I watch?

Traditional server performance monitoring works effectively for general Configuration Manager. You can also leverage the various System Center Operations Manager management packs for Configuration Manager, SQL Server, and Windows Server to monitor basic health of your servers. You can also directly monitor the Windows

Performance Monitor (PerfMon) counters Configuration Manager provides. Monitor the backlogs in the various inboxes for early warning signs of potential site performance issues or backlogs.

See also

- Site sizing and performance guidelines
- Configuration Manager on Azure frequently asked questions

Frequently asked questions about diagnostics and usage data for System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article provides answers to frequently asked questions about diagnostic and usage data in Configuration Manager.

FAQs

How do I turn off telemetry?

Telemetry can't be turned off. However, you can choose the level of telemetry data that's collected. To help manage when telemetry data is submitted, use the service connection point in offline mode.

The current branch of Configuration Manager needs to be updated on a regular basis to support new versions of Windows 10 and Microsoft Intune. Microsoft requires at least the basic level of diagnostic and usage data. This data is used to keep the product up-to-date, improve the update experience, and improve the quality and security of the product.

What is the data retention period?

Diagnostic and usage data is stored for one year.

Is diagnostics and usage data sent when installing or updating the product?

No. Diagnostics and usage data is only sent after the site is installed and operational.

How frequently is the data sent?

The SQL stored procedures run every seven days from the date the site is installed. In online mode, the service connection point is configured to upload the data after the queries run. In offline mode, the administrator uses the service connection tool to upload the data. (The data isn't initially available for offline use until seven days after the site is installed.)

Can the data be used to form a network map?

As shown in the description of the levels of diagnostic and usage data, site details include time zone information from each site. This information can provide insight into the broad geolocation and global dispersion of sites in a hierarchy. This data doesn't include any network details, such as IP addresses or more detailed geographic information. For more information, see the list of diagnostics and usage data articles, and find the levels of diagnostic and usage data collection for the version you're using.

Can you see data in custom tables?

No. Configuration Manager collects diagnostics and usage data via SQL stored procedures. These stored procedures run against default product tables in the database. All of these SQL tables are prefixed with **TEL_**. As part of the SQL schema detection query, all table names are hashed for comparison against the known defaults. This behavior determines that custom tables exist in the database. The presence of custom tables informs that the database schema is extended from the default. It doesn't include any of the data stored within those tables.

Can you see names of other databases, or can you see data in other databases?

No. The stored procedures to collect data are limited to the site database.

Is Configuration Manager subject to the General Data Protection Regulation (GDPR)?

No. Configuration Manager isn't subject to GDPR oversight. It is an on-premises product that you directly deploy, manage, and operate. The diagnostics and usage data that Microsoft collects improves the installation experience, quality, and security of future releases. This diagnostics and usage data is subject to GDPR oversight. However, no end-user identification information (EUII) or end-user pseudonymous identifiers (EUPI) are collected and transmitted to Microsoft. For more information about GDPR, see the Microsoft Trust Center on GDPR. For more information about Configuration Manager data, see Diagnostics and usage data.

See also

Diagnostics and usage data

Get ready for System Center Configuration Manager

7/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the information in the following topics when you're ready to start planning your System Center Configuration Manager deployment:

- Design a hierarchy of sites for System Center Configuration Manager
- Fundamentals of role-based administration for System Center Configuration Manager
- Fundamental concepts for content management in System Center Configuration Manager
- Understand how clients find site resources and services for System Center Configuration Manager
- Prepare your network environment for System Center Configuration Manager
- Supported configurations for System Center Configuration Manager

Features and capabilities of Configuration Manager

5/13/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article summarizes the primary management features of Configuration Manager. Each feature has its own prerequisites, and how you use each might influence the design and implementation of your Configuration Manager hierarchy. For example, if you want to deploy software updates to devices in your hierarchy, you need a software update point site system role.

For more information about how to plan and install Configuration Manager to support these management capabilities in your environment, see Get ready for Configuration Manager.

Co-management

Co-management is one of the primary ways to attach your existing Configuration Manager deployment to the Microsoft 365 cloud. It enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune. Co-management lets you cloud-attach your existing investment in Configuration Manager by adding new functionality like conditional access. For more information, see What is co-management?.

Cloud-attached management

Use features like the cloud management gateway, cloud-based distribution points, and Azure Active Directory to manage internet-based clients.

For more information, see the following articles:

- Manage clients on the internet
- Plan for Azure AD
- Azure services

Real-time management

Use CMPivot to immediately query online devices, then filter and group the data for deeper insights. Also use the Configuration Manager console to manage and deploy Windows PowerShell scripts to clients. For more information, see CMPivot and Create and run PowerShell scripts.

Application management

Helps you create, manage, deploy, and monitor applications to a range of different devices that you manage. Deploy, update, and manage Office 365 from the Configuration Manager console. Additionally, Configuration Manager integrates with the Microsoft Store for Business and Education to deliver cloud-based apps. For more information, see Introduction to application management.

OS deployment

Deploy an in-place upgrade of Windows 10, or capture and deploy OS images. Image deployment can use PXE, multicast, or bootable media. It can also help redeploy existing devices using Windows AutoPilot. For more information, see Introduction to OS deployment.

Software updates

Manage, deploy, and monitor software updates in the organization. Integrate with Windows Delivery Optimization and other peer caching technologies to help control network usage. For more information, see Introduction to software updates.

Company resource access

Lets you give users in your organization access to data and applications from remote locations. This feature includes Wi-Fi, VPN, email, and certificate profiles. For more information, see Protect data and site infrastructure.

Compliance settings

Helps you to assess, track, and remediate the configuration compliance of client devices in the organization. Additionally, you can use compliance settings to configure a range of features and security settings on devices you manage. For more information, see Ensure device compliance.

Endpoint Protection

Provides security, antimalware, and Windows Firewall management for computers in your organization. This area includes management and integration with the following Windows Defender suite features:

- Windows Defender Antivirus
- Microsoft Defender Advanced Threat Protection
- Windows Defender Exploit Guard
- Windows Defender Application Guard
- Windows Defender Application Control
- Windows Defender Firewall

For more information, see Endpoint Protection.

Inventory

Helps you identify and monitor assets.

Hardware inventory

Collects detailed information about the hardware of devices in your organization. For more information, see Introduction to hardware inventory.

Software inventory

Collects and reports information about the files that are stored on client computers in your organization. For more information, see Introduction to software inventory.

Asset Intelligence

Provides tools to collect inventory data and monitor software license usage in your organization. For more information, see Introduction to Asset Intelligence.

On-premises mobile device management

Enrolls and manages devices by using the on-premises Configuration Manager infrastructure with the management functionality built into the device platforms. (Typical management uses a separately installed Configuration Manager client.) This feature currently supports managing Windows 10 Enterprise and Windows 10 Mobile devices. For more information, see Manage mobile devices with on-premises infrastructure.

Power management

Manage and monitor the power consumption of client computers in the organization. Configure power plans, and use Wake-on-LAN to do maintenance outside of business hours. For more information, see Introduction to power management.

Remote control

Provides tools to remotely administer client computers from the Configuration Manager console. For more information, see Introduction to remote control.

Reporting

Use the advanced reporting capabilities of SQL Server Reporting Services from the Configuration Manager console. This feature provides hundreds of default reports. For more information, see Introduction to reporting.

Software metering

Monitor and collect software usage data from Configuration Manager clients. You can use this data to determine whether software is used after it's installed. For more information, see Monitor app usage with software metering.

What's changed in System Center Configuration Manager from System Center 2012 Configuration Manager

9/11/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The current branch of Configuration Manager introduces important changes from System Center 2012 Configuration Manager. This article identifies significant changes and new capabilities found in the baseline version 1511 of System Center Configuration Manager. To learn about changes introduced in subsequent updates for System Center Configuration Manager, see What's new in System Center Configuration Manager incremental versions.

The December 2015 release of System Center Configuration Manager (version 1511) was the initial release of the current Configuration Manager product from Microsoft. It's typically referred to as System Center Configuration Manager current branch. *Current branch* indicates this version supports incremental updates to the product. It also provides a way to distinguish between this release and previous releases of Configuration Manager.

System Center Configuration Manager:

- Doesn't use a year or product identifier in the product name, unlike past versions such as Configuration Manager 2007 or System Center 2012 Configuration Manager.
- Supports incremental, in-product updates, also called update versions. The initial release was version 1511. Subsequent versions are released several times a year as in-console updates, like version 1810.
- Is installed using a baseline version. While 1511 was the original baseline version, new baseline versions are also released from time to time, like 1902. Baseline versions can be used to install a new System Center Configuration Manager site and hierarchy or to upgrade from a supported version of Configuration Manager 2012.

In-console updates for Configuration Manager

System Center Configuration Manager uses an in-console service method called **Updates and Servicing** that makes it easy to locate and install recommended updates.

Some versions are only available as updates for existing sites (from within the Configuration Manager console), and can't be used to install new Configuration Manager sites. For example, the 1810 update is only available from within the Configuration Manager console. It's used to update a site that already runs a version of System Center Configuration Manager.

Periodically, an update version is also released as a new baseline version (like update 1902). This kind of update can be used to install a new hierarchy, without the need to start with an older baseline version (like 1802) and upgrade your way to the most current version.

For more information about using updates, see Updates for Configuration Manager.
For more information about baselines, see Baseline and update versions.

New site system role: service connection point

The **Microsoft Intune connector** is replaced by a new site system role that enables additional functionality, the

service connection point. The service connection point:

- Replaces the Microsoft Intune connector when you integrate Intune with System Center Configuration Manager on-premises mobile device management.
- Is used as a point-of-contact for devices you manage.
- Uploads usage data about your deployment to the Microsoft cloud service.
- Makes updates that apply to your deployment available from within the Configuration Manager console.

This site system role supports both online and offline modes of operation. For more information, see About the service connection point.

Usage data collection

Configuration Manager collects usage data about your sites and infrastructure. This information is compiled and submitted to the Microsoft cloud service by the service connection point. It's required to enable Configuration Manager to download updates for your deployment that apply to the version of Configuration Manager you use. When you set up the service connection point, you can specify both the level of data that is collected, and whether the data is submitted automatically (online mode) or manually (offline mode).

For more information, see Diagnostics and usage data.

Support for Intel Active Management Technology (AMT)

Configuration Manager current branch removes native support for AMT-based computers from within the Configuration Manager console. AMT-based computers remain fully managed when you use the Intel SCS Add-on for Microsoft System Center Configuration Manager. The add-on provides you access to the latest capabilities to manage AMT, while removing limitations introduced until Configuration Manager could incorporate those changes.

The removal of integrated AMT for Configuration Manager includes out-of-band management. The out-of-band management point site system role is no longer available.

> **NOTE**
> Out-of-band management in System Center 2012 Configuration Manager isn't affected by this change.

Deprecated functionality

Some features, like native Support for Intel Active Management Technology (AMT) based-computers, are removed from the Configuration Manager console. Other features, like Network Access Protection, are removed entirely. Additionally, some older Microsoft products like Windows Vista, Windows Server 2008, and SQL Server 2008, are no longer supported.

For a list of deprecated features, see Removed and deprecated items.

For details about supported products, operating systems, and configurations, see Supported configurations.

Client deployment

Configuration Manager introduces a new feature for testing new versions of the Configuration Manager client before upgrading the rest of site with the new software. You can set up a pre-production collection in which to pilot a new client. Once you're satisfied with the new client software in pre-production, you can promote the client to automatically upgrade the rest of the site with the new version.

For more information on how to test clients, see How to test client upgrades in a pre-production collection.

OS deployment

Be aware of the following changes to OS deployment:

- In the Create Task Sequence Wizard, a new task sequence type is available: **Upgrade an operating system from upgrade package**. It creates the steps to upgrade computers from Windows 7, Windows 8, or Windows 8.1 to Windows 10. For more information, see Upgrade Windows to the latest version.
- Windows PE peer cache is now available when you deploy operating systems. Computers that run a task sequence to deploy an OS can use Windows PE peer cache to obtain content from a peer cache source, instead of downloading content from a distribution point. This behavior helps minimize WAN traffic in branch office scenarios where there's no local distribution point. For more information, see Prepare Windows PE peer cache to reduce WAN traffic.
- You can now view the state of Windows as a service in your environment. You can also create servicing plans to form deployment rings, and make sure that Windows 10 current branch computers are kept up-to-date when new builds are released. Additionally, you can view alerts when Windows 10 clients are near the end of support for their build. For more information, see Manage Windows as a service.

Application management

Be aware of the following changes to application management:

- Configuration Manager lets you deploy Universal Windows Platform (UWP) apps for devices running Windows 10 and later. For more information, see Creating Windows applications.
- Software Center has a new, modern look. User-available apps that previously only appeared in the application catalog now appear in Software Center under the Applications tab. This behavior makes these deployments more discoverable, and makes it unnecessary for users to refer to the application catalog. Additionally, a Silverlight-enabled browser is no longer required. For more information, see Plan for and configure application management.
- The new Windows Installer through MDM application type lets you create and deploy Windows Installer-based apps to enrolled PCs that run Windows 10. For more information, see Creating Windows applications.
- When you create an application for an in-house iOS app, you only need to specify the installer (.ipa) file for the app. You no longer need to specify a corresponding property list (.plist) file. See Creating iOS applications.
- In Configuration Manager 2012, to specify a link to an app in the Windows Store, you could either specify the link directly, or browse to a remote computer that had the app installed. In Configuration Manager current branch, you can still enter the link directly, but now, instead of browsing to a reference computer, you can browse the store for the app directly from the Configuration Manager console.

Software updates

Be aware of the following changes to software updates:

- Configuration Manager can now detect the difference between software update management methods for computers. Specifically, it can differentiate between a Windows 10 computer that connects to Windows Update for Business (WUfB), and a computer connected to WSUS. The **UseWUServer** attribute is new, and specifies whether the computer is managed with WUfB. You can use this setting in a collection to remove these computers from software update management. For more information, see Integration with

Windows Update for Business in Windows 10.

- You can now schedule and run the WSUS clean-up task from the Configuration Manager console. In **Software Update Point Component** properties, when you select to run the WSUS clean-up task, it runs at the next software updates synchronization. The expired software updates are set to a status of declined on the WSUS server, and the Windows Update Agent on computers no longer scans these software updates. For more information, see Schedule and run the WSUS clean up task.

Compliance settings

Be aware of the following changes to compliance settings:

- Configuration Manager improves the workflow for creating configuration items. Now, when you create a configuration item, and select supported platforms, only the settings relevant to that platform are available. See Get started with compliance settings.
- The **Create Configuration Item** wizard now makes it easier to choose the configuration item type you want to create. Additionally, new and updated configuration items are available for:
  - Windows 10 devices managed with the Configuration Manager client
  - Mac OS X devices managed with the Configuration Manager client
  - Windows desktop and server computers managed with the Configuration Manager client
  - Windows 8.1 and Windows 10 devices managed without the Configuration Manager client
  - Windows Phone devices managed without the Configuration Manager client
  - iOS and Mac OS X devices managed without the Configuration Manager client
  - Android and Samsung KNOX Standard devices managed without the Configuration Manager client

  For more information, see How to create configuration items.
- Support for managing settings on Mac OS X computers that are either enrolled with Microsoft Intune or managed with the Configuration Manager client. See How to create configuration items for iOS and Mac OS X devices managed without the Configuration Manager client.

On-premises mobile device management

You can now manage mobile devices by using on-premises Configuration Manager infrastructure. All device and management data are handled on-premises, and isn't part of Microsoft Intune or other cloud services. This type of device management doesn't require client software. Configuration Manager manages devices with functionality that's built into the device OS.

For more information, see Manage mobile devices with on-premises infrastructure.

What's new in Configuration Manager incremental versions

7/26/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager uses an in-console updates and servicing process. This update process makes it easy to discover and install Configuration Manager updates. There are no more service packs or cumulative update versions to track and install. You don't have to search for the download of the most recent release or updates.

To update the product to a new version of the current branch, use the Configuration Manager console to find and then install in-console updates. A few times each year, Microsoft releases new versions that include product updates. Each version also introduces new features. When you install an update with new features, you can choose to use those features.

Different update versions are identified by year and month. For example, version 1511 identifies November 2015 (the month when Configuration Manager current branch was first released to manufacturing). Later updates have version names like 1802, which indicates an update that was created in February 2018. These update versions are key to understanding the incremental version of your Configuration Manager installation, and what features are available to enable in your environment.

Supported versions

Use the following links to discover what's new with each supported version:

- What's new in version 1906
- What's new in version 1902
- What's new in version 1810
- What's new in version 1806
- What's new in version 1802

Each update version remains in support for 18 months from its general availability (GA) release date. Stay current with the most recent update version. For more information, see Support for Configuration Manager current branch versions.

See also

Release notes

What's new in version 1906 of Configuration Manager current branch

8/23/2019 • 23 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Update 1906 for Configuration Manager current branch is available as an in-console update. Apply this update on sites that run version 1802 or later. This article summarizes the changes and new features in Configuration Manager, version 1906.

Always review the latest checklist for installing this update. For more information, see Checklist for installing update 1906. After you update a site, also review the Post-update checklist.

To take full advantage of new Configuration Manager features, after you update the site, also update clients to the latest version. While new functionality appears in the Configuration Manager console when you update the site and console, the complete scenario isn't functional until the client version is also the latest.

TIP

To get notified when this page is updated, copy and paste the following URL into your RSS feed reader:

```
https://docs.microsoft.com/api/search/rss?search=%22what%27s+new+in+version+1906+-
+Configuration+Manager%22&locale=en-us
```

Requirement changes

Version 1906 client requires SHA-2 code signing support

Because of weaknesses in the SHA-1 algorithm and to align to industry standards, Microsoft now only signs Configuration Manager binaries using the more secure SHA-2 algorithm. The following Windows OS versions require an update for SHA-2 code signing support:

- Windows 7 SP1
- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2

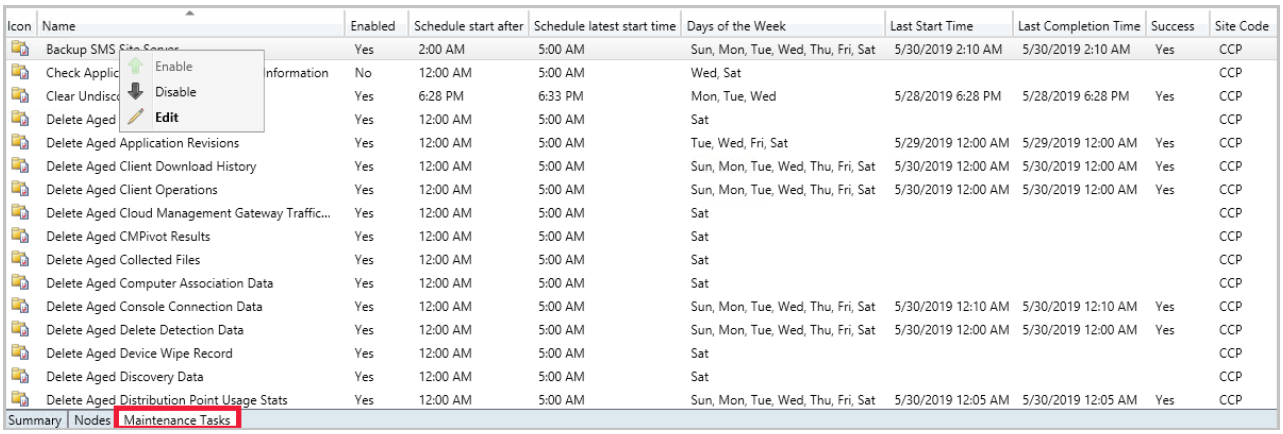
For more information, see Prerequisites for Windows clients.

Site infrastructure

Site server maintenance task improvements

Site server maintenance tasks can now be viewed and edited from their own tab on the details view of a site server. The new **Maintenance Tasks** tab gives you information such as:

- If the task is enabled
- The task schedule
- Last start time
- Last completion time
- If the task completed successfully

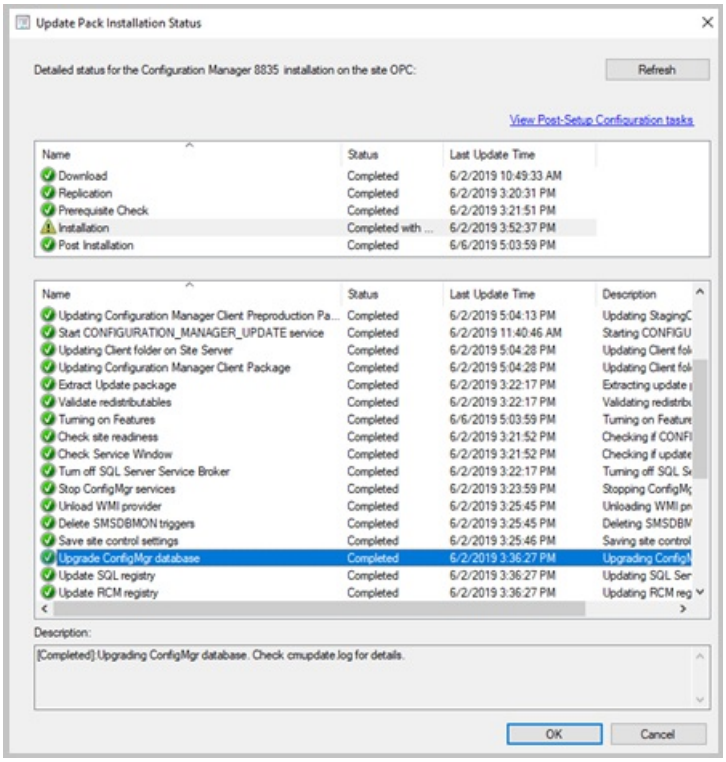


For more information, see Maintenance tasks.

Configuration Manager update database upgrade monitoring

When applying a Configuration Manager update, you can now see the state of the **Upgrade ConfigMgr database** task in the installation status window.

- If the database upgrade is blocked, then you'll be given the warning, **In progress, needs attention**.
  - The cmupdate.log will log the program name and sessionid from SQL that is blocking the database upgrade.
- When the database upgrade is no longer blocked, the status will be reset to **In progress** or **Complete**.
  - When the database upgrade is blocked, a check is done every 5 minutes to see if it's still blocked.



For more information, see Install in-console updates.

Management insights rule for NTLM fallback

Management insights includes a new rule that detects if you enabled the less secure NTLM authentication fallback method for the site: **NTLM fallback is enabled**.

For more information, see Management insights.

Improvements to support for SQL Always On

- Add a new synchronous replica from setup: You can now add a new secondary replica node to an existing

SQL Always On availability group. Instead of a manual process, use Configuration Manager setup to make this change. For more information, see Configure SQL Server Always On availability groups.

- Multi-subnet failover: You can now enable the MultiSubnetFailover connection string keyword in SQL Server. You also need to manually configure the site server. For more information, see the Multi-subnet failover prerequisite.
- Support for distributed views: The site database can be hosted on a SQL Server Always On availability group, and you can enable database replication links to use distributed views.

  > **NOTE**
  > This change doesn't apply to SQL Server clusters.

- Site recovery can recreate the database on a SQL Always On group. This process works with both manual and automatic seeding.
- New setup prerequisite checks:
  - SQL availability group replicas must all have the same seeding mode
  - SQL availability group replicas must be healthy

Cloud-attached management

Azure Active Directory user group discovery

You can now discover user groups and members of those groups from Azure Active Directory (Azure AD). Users found in Azure AD groups that the site hasn't previously discovered are added as user resources in Configuration Manager. A user group resource record is created when the group is a security group. This feature is a pre-release feature and needs to be enabled.

For more information, see Configure discovery methods.

Synchronize collection membership results to Azure Active Directory groups

You can now enable the synchronization of collection memberships to an Azure Active Directory (Azure AD) group. This synchronization is a pre-release feature. To enable it, see Pre-release features.

The synchronization allows you to use your existing on-premises grouping rules in the cloud by creating Azure AD group memberships based on collection membership results. Only devices with an Azure Active Directory record are reflected in the Azure AD Group. Both Hybrid Azure AD Joined and Azure Active Directory joined devices are supported.

For more information, see Create collections.

Desktop Analytics

Readiness insights for desktop apps

You can now get more detailed insights for your desktop applications including line-of-business apps. The former App Health Analyzer toolkit is now integrated with the Configuration Manager client. This integration simplifies deployment and manageability of app readiness insights in the Desktop Analytics portal.

For more information, see Compatibility assessment in Desktop Analytics.

DALogsCollector tool

Use the DesktopAnalyticsLogsCollector.ps1 tool from the Configuration Manager install directory to help troubleshoot Desktop Analytics. It runs some basic troubleshooting steps and collects the relevant logs into a single working directory.

For more information, see Logs collector.

Real-time management

Add joins, additional operators, and aggregators in CMPivot

For CMPivot, you now have additional arithmetic operators, aggregators, and the ability to add query joins such as using Registry and File together.

For more information, see CMPivot.

CMPivot standalone

You can now use CMPivot as a standalone app. CMPivot standalone is a **pre-release feature** and is only available in English. Run CMPivot outside of the Configuration Manager console to view the real-time state of devices in your environment. This change enables you to use CMPivot on a device without first installing the console.

You can share the power of CMPivot with other personas, such as helpdesk or security admins, who don't have the console installed on their computer. These other personas can use CMPivot to query Configuration Manager alongside the other tools that they traditionally use. By sharing this rich management data, you can work together to proactively solve business problems that cross roles.

For more information, see CMPivot and Pre-release features.

Added permissions to the Security Administrator role

The following permissions have been added to Configuration Manager's built-in **Security Administrator** role:

- Read on SMS Script
- Run CMPivot on Collection
- Read on Inventory Report

For more information, see CMPivot.

Content management

Delivery Optimization download data in client data sources dashboard

The client data sources dashboard now includes Delivery Optimization data. This dashboard helps you understand from where clients are getting content in your environment.

For more information, see Client Data Sources dashboard.

Use your distribution point as an in-network cache server for Delivery Optimization

You can now install Delivery Optimization In-Network Cache (DOINC) server on your distribution points. By caching this content on-premises, your clients can benefit from the Delivery Optimization feature, but you can help to protect WAN links.

This cache server acts as an on-demand transparent cache for content downloaded by Delivery Optimization. Use client settings to make sure this server is offered only to the members of the local Configuration Manager boundary group.

For more information, see Delivery Optimization In-Network Cache in Configuration Manager.

Client management

Support for Windows Virtual Desktop

Windows Virtual Desktop is a preview feature of Microsoft Azure and Microsoft 365. You can now use Configuration Manager to manage these virtual devices running Windows in Azure.

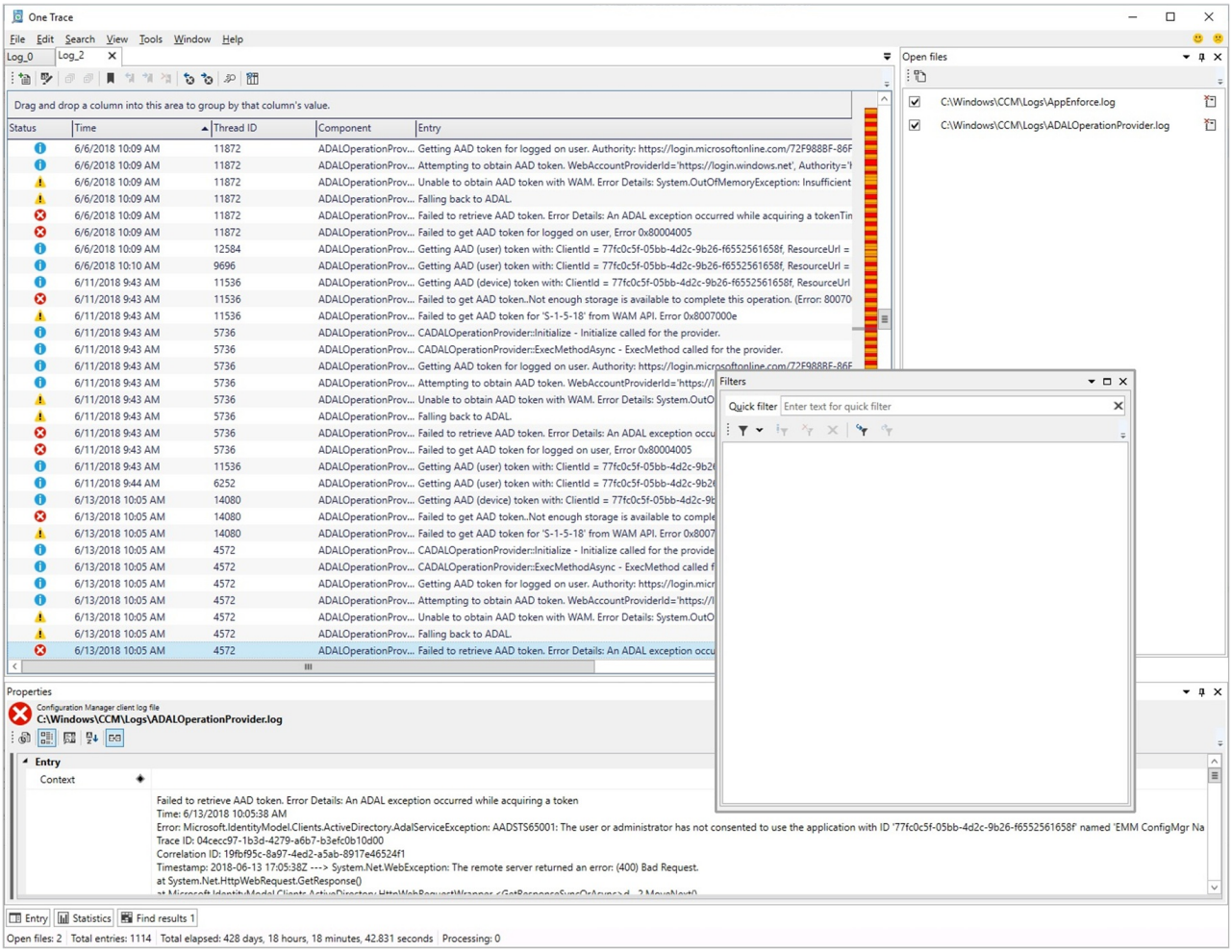
Similar to a terminal server, these virtual devices allow multiple concurrent active user sessions. To help with client performance, Configuration Manager now disables user policies on any device that allows these multiple user sessions. Even if you enable user policies, the client disables them by default on these devices, which include Windows Virtual Desktop and terminal servers.

For more information, see Supported OS versions for clients and devices.

Support Center OneTrace (Preview)

OneTrace is a new log viewer with Support Center. It works similarly to CMTrace, with the following improvements:

- A tabbed view
- Dockable windows
- Improved search capabilities
- Ability to enable filters without leaving the log view
- Scrollbar hints to quickly identify clusters of errors
- Fast log opening for large files



For more information, see Support Center OneTrace.

Configure client cache minimum retention period

You can now specify the minimum time for the Configuration Manager client to keep cached content. This client setting defines the minimum amount of time Configuration Manager agent should wait before it can remove content from the cache in case more space is needed. In the **Client cache settings** group of client settings, configure the following setting: **Minimum duration before cached content can be removed (minutes)**.

> **NOTE**
> In the same client setting group, the existing setting to **Enable Configuration Manager client in full OS to share content** is now renamed to **Enable as peer cache source**. The behavior of the setting doesn't change.

For more information, see Client cache settings.

Co-management

Improvements to co-management auto-enrollment

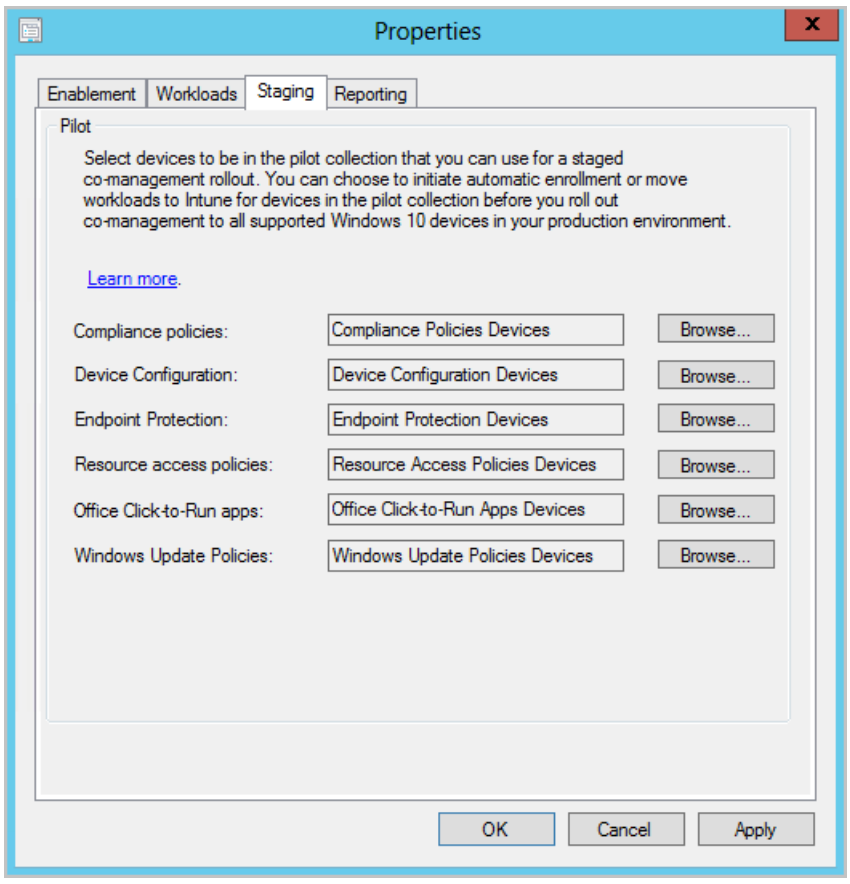
- A new co-managed device now automatically enrolls to the Microsoft Intune service based on its Azure Active Directory (Azure AD) *device* token. It doesn't need to wait for a user to sign in to the device for auto-enrollment to start. This change helps to reduce the number of devices with the enrollment status *Pending user sign in*.
- For customers that already have devices enrolled to co-management, new devices now enroll immediately once they meet the prerequisites. For example, once the device is joined to Azure AD and the Configuration Manager client is installed.

For more information, see Enable co-management.

Multiple pilot groups for co-management workloads

You can now configure different pilot collections for each of the co-management workloads. Using different pilot collections allows you to take a more granular approach when shifting workloads.

- In the **Enablement** tab, you can now specify an **Intune Auto Enrollment** collection.
  - The **Intune Auto Enrollment** collection should contain all of the clients you want to onboard into co-management. It's essentially a superset of all the other staging collections.
- In the **Staging** tab, instead of using one pilot collection for all workloads, you can now choose an individual collection for each workload.



These options are also available when you first enable co-management.

For more information, see Enable co-management.

Co-management support for government cloud

U.S. government customers can now use co-management with the Azure U.S. Government Cloud (portal.azure.us). For more information, see Enable co-management.

Application management

Filter applications deployed to devices

User categories for device-targeted application deployments now show as filters in Software Center. Specify a **user category** for an application on the **Software Center** page of its properties. Then open the app in Software Center and look at the available filters.

For more information, see Manually specify application information.

Application groups

Create a group of applications that you can send to a user or device collection as a single deployment. The metadata you specify about the app group is seen in Software Center as a single entity. You can order the apps in the group so that the client installs them in a specific order.

This feature is pre-release. To enable it, see Pre-release features.

For more information, see Create application groups.

Retry the install of pre-approved applications

You can now retry the installation of an app that you previously approved for a user or device. The approval option is only for available deployments. If the user uninstalls the app, or if the initial install process fails, Configuration Manager doesn't reevaluate its state and reinstall it. This feature allows a support technician to quickly retry the app install for a user that calls for help.

For more information, see Approve applications.

Install an application for a device

From the Configuration Manager console, you can now install applications to a device in real time. This feature can help reduce the need for separate collections for every application.

For more information, see Install applications for a device.

Improvements to app approvals

This release includes the following improvements to app approvals:

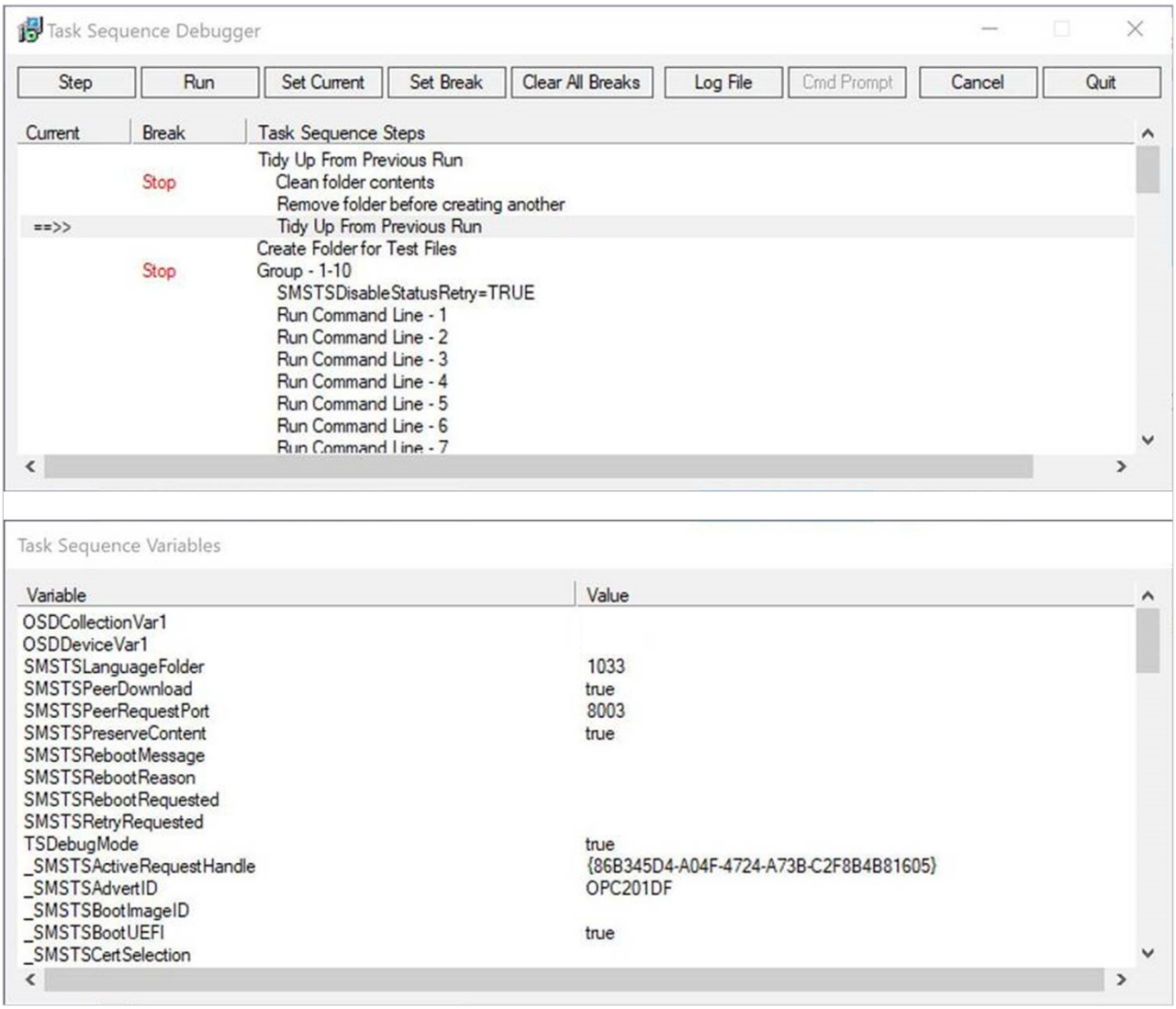
- If you approve an app request in the console, and then deny it, you can now approve it again. The app is reinstalled on the client after you approve it.
- In the Configuration Manager console, **Software Library** workspace, under **Application Management**, the **Approval Requests** node is renamed **Application Requests**.
- There's a new WMI method, **DeleteInstance** to remove an app approval request. This action doesn't uninstall the app on the device. If it's not already installed, the user can't install the app from Software Center.
- Call the **CreateApprovedRequest** API to create a pre-approved request for an app on a device. To prevent automatically installing the app on the client, set the **AutoInstall** parameter to `FALSE`. The user sees the app in Software Center, but it's not automatically installed.

For more information, see Approve applications.

OS deployment

Task sequence debugger

The task sequence debugger is a new troubleshooting tool. You deploy a task sequence in debug mode to a collection of one device. It lets you step through the task sequence in a controlled manner to aid troubleshooting and investigation.



This feature is pre-release. To enable it, see Pre-release features.

For more information, see Debug a task sequence.

Clear app content from client cache during task sequence

In the **Install Application** task sequence step, you can now delete the app content from the client cache after the step runs.

For more information, see About task sequence steps.

> **IMPORTANT**
> Update the target client to the latest version to support this new feature.

Reclaim SEDO lock for task sequences

If the Configuration Manager console stops responding, you can be locked out of making further changes to a task

sequence. Now when you attempt to access a locked task sequence, you can now **Discard Changes**, and continue editing the object.

For more information, see Manage task sequences.

Pre-cache driver packages and OS images

Task sequence pre-cache now includes additional content types. Pre-cache content previously only applied to OS upgrade packages. Now you can use pre-caching to reduce bandwidth consumption of:

- OS images
- Driver packages
- Packages

For more information, see Configure pre-cache content.

Improvements to OS deployment

This release includes the following improvements to OS deployment:

- Use the following two PowerShell cmdlets to create and edit the Run Task Sequence step:
  - **New-CMTSStepRunTaskSequence**
  - **Set-CMTSStepRunTaskSequence**
- It's now easier to edit variables when you run a task sequence. After you select a task sequence in the Task Sequence Wizard window, the page to edit task sequence variables includes an **Edit** button. For more information, see How to use task sequence variables.
- The **Disable BitLocker** task sequence step has a new restart counter. Use this option to specify the number of restarts to keep BitLocker disabled. This change helps you simplify your task sequence. You can use a single step, instead of adding multiple instances of this step. For more information, see Disable BitLocker.
- Use the new task sequence variable **SMSTSRebootDelayNext** with the existing SMSTSRebootDelay variable. If you want any later reboots to happen with a different timeout than the first, set this new variable to a different value in seconds. For more information, see SMSTSRebootDelayNext.
- The task sequence sets a new read-only variable **_SMSTSLastContentDownloadLocation**. This variable contains the last location where the task sequence downloaded or attempted to download content. Inspect this variable instead of parsing the client logs.

Software Center

Improvements to Software Center tab customizations

You can now add up to five custom tabs in Software Center. You can also edit the order in which these tabs appear in Software Center.

For more information, see Software Center client settings.

Software Center infrastructure improvements

This release includes the following infrastructure improvements to Software Center:

- Software Center now communicates with a management point for apps targeted to users as available. It doesn't use the application catalog anymore. This change makes it easier for you to remove the application catalog from the site.
- Previously, Software Center picked the first management point from the list of available servers. Starting in this release, it uses the same management point that the client uses. This change allows Software Center to use the same management point from the assigned primary site as the client.

> **IMPORTANT**
>
> These iterative improvements to Software Center and the management point are to retire the application catalog roles.
>
> - The Silverlight user experience isn't supported as of current branch version 1806.
> - Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles.
> - In the first current branch release after October 31, 2019, support will end for the application catalog roles.

For more information, see Remove the application catalog and Plan for Software Center.

Redesigned notification for newly available software

The **New Software is Available** notification will only show once for a user for a given application and revision. The user will no longer see the notification each time they sign in. They'll only see another notification for an application if it has changed or was redeployed.

For more information, see Create and deploy an application.

More frequent countdown notifications for restarts

End users will now be reminded more frequently of a pending restart with intermittent countdown notifications. You can define the interval for the intermittent notifications in **Client Settings** on the **Computer Restart** page. Change the value for **Specify the snooze duration for computer restart countdown notifications (minutes)** to configure how often a user is reminded about a pending restart until the final countdown notification occurs.

Additionally, the maximum value for **Display a temporary notification to the user that indicates the interval before the user is logged off or the computer restarts (minutes)** increased from 1440 minutes (24 hours) to 20160 minutes (two weeks).

For more information, see Device restart notifications and About client settings.

Direct link to custom tabs in Software Center

You can now provide users with a direct link to a custom tab in Software Center.

Use the following URL format to open Software Center to a particular tab:

```
softwarecenter:page=CustomTab1
```

The string `CustomTab1` is the first custom tab in order.

For example, type this URL in the Windows **Run** window.

You can also use this syntax to open default tabs in Software Center:

COMMAND LINE	TAB
`AvailableSoftware`	Applications
`Updates`	Updates
`OSD`	Operating Systems
`InstallationStatus`	Installation status
`Compliance`	Device compliance

COMMAND LINE	TAB
`Options`	Options

For more information, see Software Center tab visibility.

Software updates

Additional options for WSUS maintenance

You now have additional WSUS maintenance tasks that Configuration Manager can run to maintain healthy software update points. The WSUS maintenance occurs after every synchronization. In addition to declining expired updates in WSUS, Configuration Manager can now:

- Remove obsolete updates from the WSUS database.
- Add non-clustered indexes to the WSUS database to improve WSUS cleanup performance.

For more information, see Software updates maintenance.

Configure the default maximum run time for software updates

You can now specify the maximum amount of time a software update installation has to complete. You can specify the following items in the **Maximum Run Time** tab on the Software Update Point:

- **Maximum run time for Windows feature updates (minutes)**
- **Maximum run time for Office 365 updates and non-feature updates for Windows (minutes)**

For more information, see Plan for software updates.

Configure dynamic update during feature updates

Use a new client setting to configure Dynamic Update during Windows 10 feature update installs. Dynamic Update installs language packs, features on demand, drivers, and cumulative updates during Windows setup by directing the client to download these updates from the internet.

For more information, see Software update client settings and Manage Windows as a service.

New Windows 10, version 1903 and later product category

Windows 10, version 1903 and later was added to Microsoft Update as its own product rather than being part of the **Windows 10** product like earlier versions. This change caused you to do a number of manual steps to ensure that your clients see these updates. We've helped reduce the number of manual steps you have to take for the new product.

When you update to Configuration Manager version 1906 and have the **Windows 10** product selected for synchronization, the following actions occur automatically:

- The **Windows 10, version 1903 and later** product is added for synchronization.
- Automatic Deployment Rules containing the **Windows 10** product will be updated to include **Windows 10, version 1903 and later**.
- Servicing plans are updated to include the **Windows 10, version 1903 and later** product.

For more information, see Configure classifications and products to synchronize, Servicing plans, and Automatic deployment rules.

Drill through required updates

You can now drill through compliance statistics to see which devices require a specific software update. To view the device list, you need permission to view updates and the collections the devices belong to. To drill down into the device list, select the **View Required** hyperlink next to the pie chart in the **Summary** tab for an update. Clicking

the hyperlink takes you to a temporary node under **Devices** where you can see the devices requiring the update.

The **View Required** hyperlink is available in the following locations:

- **Software Library** > **Software Updates** > **All Software Updates**
- **Software Library** > **Windows 10 Servicing** > **All Windows 10 Updates**
- **Software Library** > **Office 365 Client Management** > **Office 365 Updates**

For more information, see Monitor software updates, Manage Windows as a service, and Manage Office 365 ProPlus updates.

Office management

Office 365 ProPlus upgrade readiness dashboard

To help you determine which devices are ready to upgrade to Office 365 ProPlus, there's a new readiness dashboard. It includes the **Office 365 ProPlus upgrade readiness** tile that released in Configuration Manager current branch version 1902. In the Configuration Manager console, go to the **Software Library** workspace, expand **Office 365 Client Management**, and select the **Office 365 ProPlus Upgrade Readiness** node.

For more information on the dashboard, prerequisites, and using this data, see Integration for Office 365 ProPlus readiness.

Protection

Windows Defender Application Guard file trust criteria

There's a new policy setting that enables users to trust files that normally open in Windows Defender Application Guard (WDAG). Upon successful completion, the files will open on the host device instead of in WDAG.

For more information, see Create and deploy Windows Defender Application Guard policy.

Configuration Manager console

Role-based access for folders

You can now set security scopes on folders. If you have access to an object in the folder but don't have access to the folder, you'll be unable to see the object. Similarly, if you have access to a folder but not an object within it, you won't see that object. Right-click a folder, choose **Set Security Scopes**, then choose the security scopes you want to apply.

For more information, see Using the Configuration Manager console and Configure role-based administration.

Add SMBIOS GUID column to device and device collection nodes

In both the **Devices** and **Device Collections** nodes, you can now add a new column for **SMBIOS GUID**. This value is the same as the **BIOS GUID** property of the System Resource class. It's a unique identifier for the device hardware.

Administration service support for security nodes

You can now enable some nodes of the Configuration Manager console to use the administration service. This change allows the console to communicate with the SMS Provider over HTTPS instead of via WMI.

For more information, see Administration service.

> **NOTE**
>
> Starting in version 1906, the **Client Computer Communication** tab on the site properties is now called **Communication Security**.

Collections tab in devices node

In the **Assets and Compliance** workspace, go to the **Devices** node, and select a device. In the details pane, switch to the new **Collections** tab. This tab lists the collections that include this device.

> **NOTE**
>
> - This tab currently isn't available from a devices subnode under the **Device Collections** node. For example, when you select the option to **Show Members** on a collection.
> - This tab may not populate as expected for some users. To see the complete list of collections a device belongs to, you must have the **Full Administrator** security role. This is a known issue.

Task sequences tab in applications node

In the **Software Library** workspace, expand **Application Management**, go to the **Applications** node, and select an application. In the details pane, switch to the new **Task sequences** tab. This tab lists the task sequences that reference this application.

Show collection name for scripts

In the **Monitoring** workspace, select the **Script Status** node. It now lists the **Collection Name** in addition to the ID.

Real-time actions from device lists

There are various ways to display a list of devices under the **Devices** node in the **Assets and Compliance** workspace.

- In the **Assets and Compliance** workspace, select the **Device Collections** node. Select a device collection, and choose the action to **Show members**. This action opens a subnode of the **Devices** node with a device list for that collection.
  - When you select the collection subnode, you can now start **CMPivot** from the Collection group of the ribbon.
- In the **Monitoring** workspace, select the **Deployments** node. Select a deployment, and choose the **View Status** action in the ribbon. In the deployment status pane, double-click the total assets to drill-through to a device list.
  - When you select a device in this list, you can now start **CMPivot** and **Run Scripts** from the Device group of the ribbon.

Order by program name in task sequence

In the **Software Library** workspace, expand **Operating Systems**, and select the **Task Sequences** node. Edit a task sequence, and select or add the Install Package step. If a package has more than one program, the drop-down list now sorts the programs alphabetically.

Correct names for client operations

In the **Monitoring** workspace, select **Client Operations**. The operation to **Switch to next Software Update Point** is now properly named.

Deprecated features and operating systems

Learn about support changes before they're implemented in removed and deprecated items.

Version 1906 drops support for the following features:

- You can't install new application catalog roles. Updated clients automatically use the management point for user-available application deployments. For more information, see Plan for Software Center.

Version 1906 deprecates support for the following products:

- Windows CE 7.0
- Windows 10 Mobile
- Windows 10 Mobile Enterprise

Other updates

As of this version, the following features are no longer pre-release:

- SMS Provider administration service
- Device Guard management

Aside from new features, this release also includes additional changes such as bug fixes. For more information, see Summary of changes in Configuration Manager current branch, version 1906.

For more information on changes to the Windows PowerShell cmdlets for Configuration Manager, see PowerShell version 1906 release notes.

Next steps

As of August 16, 2019, version 1906 is globally available for all customers to install.

When you're ready to install this version, see Installing updates for Configuration Manager and Checklist for installing update 1906.

> **TIP**
>
> To install a new site, use a baseline version of Configuration Manager.
>
> Learn more about:
>
> - Installing new sites
> - Baseline and update versions

For known, significant issues, see the Release notes.

After you update a site, also review the Post-update checklist.

What's new in version 1902 of Configuration Manager current branch

7/19/2019 • 19 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Update 1902 for Configuration Manager current branch is available as an in-console update. Apply this update on sites that run version 1802, 1806, or 1810. When installing a new site, it's also available as a baseline version. This article summarizes the changes and new features in Configuration Manager, version 1902.

Always review the latest checklist for installing this update. For more information, see Checklist for installing update 1902. After you update a site, also review the Post-update checklist.

To take full advantage of new Configuration Manager features, after you update the site, also update clients to the latest version. While new functionality appears in the Configuration Manager console when you update the site and console, the complete scenario isn't functional until the client version is also the latest.

TIP

To get notified when this page is updated, copy and paste the following URL into your RSS feed reader:

```
https://docs.microsoft.com/api/search/rss?search=%22what%27s+new+in+version+1902+-
+Configuration+Manager%22&locale=en-us
```

Deprecated features and operating systems

Learn about support changes before they're implemented in removed and deprecated items.

- The implementation for sharing content from Azure has changed. Use a content-enabled cloud management gateway by enabling the option to **Allow CMG to function as a cloud distribution point and serve content from Azure storage**. You won't be able to create a traditional cloud distribution point in the future.

Version 1902 drops support for the following products:

- Linux and UNIX as a client. Deprecation was announced with version 1802. Consider Microsoft Azure Management for managing Linux servers. Azure solutions have extensive Linux support that in most cases exceed Configuration Manager functionality, including end-to-end patch management for Linux.

Site infrastructure

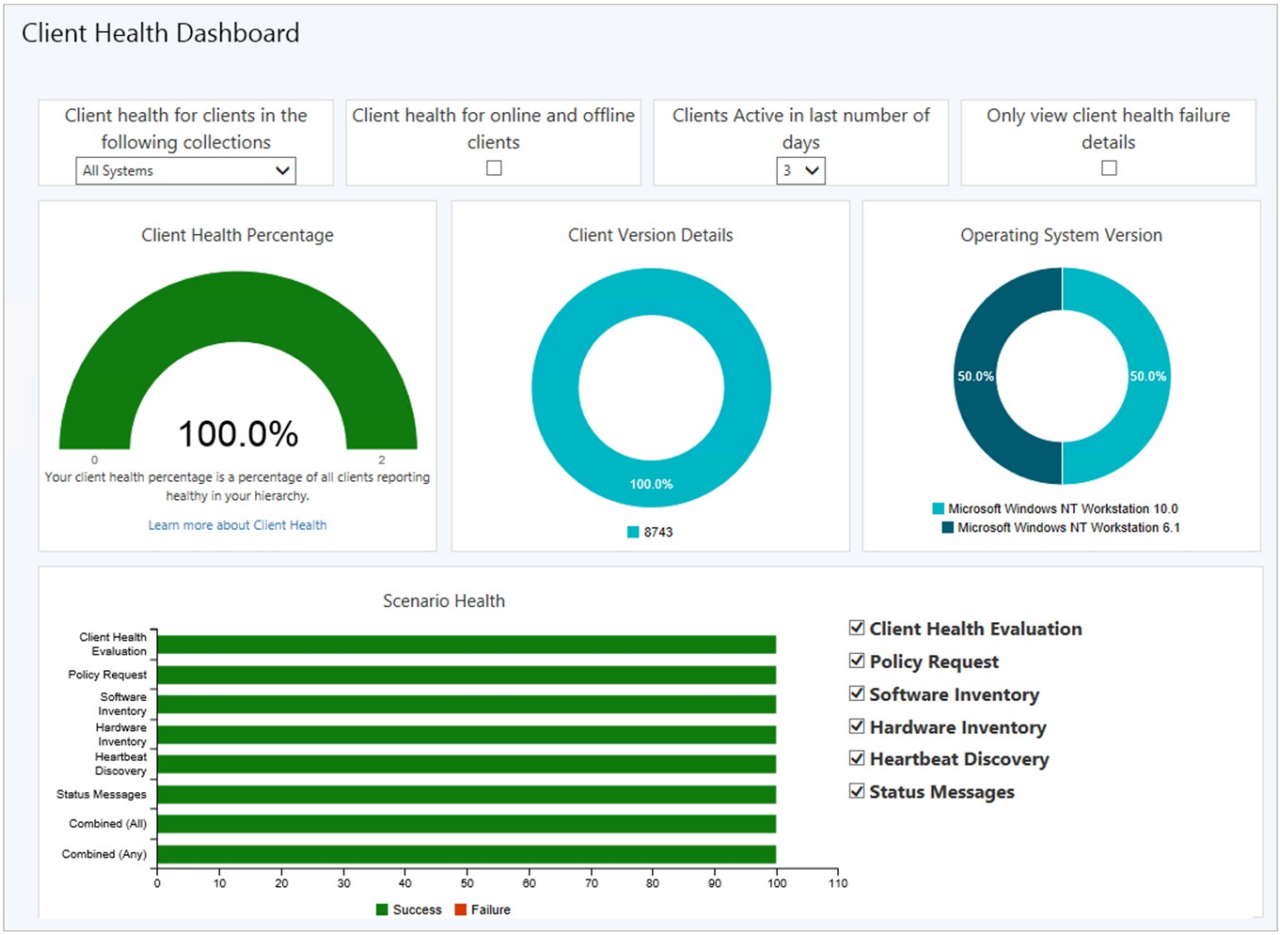
Client health dashboard

You deploy software updates and other apps to help secure your environment, but these deployments only reach healthy clients. Unhealthy Configuration Manager clients adversely effect overall compliance. Determining client health can be challenging depending upon the denominator: how many total devices should be in your scope of management? For example, if you discover all systems from Active Directory, even if some of those records are for retired machines, this process increases your denominator.

You can now view a dashboard with information about the health of Configuration Manager clients in your environment. View your client health, scenario health, and common errors. Filter the view by several attributes to see any potential issues by OS and client versions.

In the Configuration Manager console, go to the **Monitoring** workspace. Expand **Client status**, and select the

Client health dashboard node.



For more information, see How to monitor clients.

New management insight rules

The management insights feature has the following new rules:

- Multiple rules with recommendations on managing collections. Use these insights to simplify management and improve performance. Review these new rules in the **Collections** group.
- **Update clients to a supported Windows 10 version** rule in the **Simplified Management** group. This rule reports on clients that are running a version of Windows 10 that's no longer supported. It also includes clients with a Windows 10 version that's near end of service (three months).

For more information, see Management insights.

Improvement to enhanced HTTP

You can now enable enhanced HTTP per primary site or for the central administration site.

On the properties of the central administration site, select the option to **Use Configuration Manager-generated certificates for HTTP site systems**. This setting only applies to site system roles in the central administration site. It isn't a global setting for the hierarchy.

For more information, see enhanced HTTP.

Improvement to setup prerequisites

When you install or update to version 1902, Configuration Manager setup now includes the following prerequisite check:

- **Pending system restart on the remote SQL Server**: This prerequisite check is similar to the **Pending system restart** rule, but it checks a remote SQL Server. For more information, see List of prerequisite checks.

Cloud-attached management

Stop cloud service when it exceeds threshold

Configuration Manager can now stop a cloud management gateway (CMG) service when the total data transfer goes over your limit. The CMG has always had alerts to trigger notifications when the usage reached warning or critical levels. To help reduce any unexpected Azure costs because of a spike in usage, this new option turns off the cloud service.

For more information, see Stop CMG when it exceeds threshold.

Use Azure Resource Manager for cloud services

Starting in version 1810, the classic service deployment in Azure was deprecated for use in Configuration Manager. That version is the last to support creation of these Azure deployments.

Existing deployments continue to work. Starting in this current branch version, Azure Resource Manager is the only deployment mechanism for new instances of the cloud management gateway and cloud distribution point.

For more information, see Azure Resource Manager for the cloud management gateway.

Add cloud management gateway to boundary groups

You can now associate a cloud management gateway (CMG) with a boundary group. This configuration allows clients to default or fallback to the CMG for client communication according to boundary group relationships. This behavior is especially useful in branch office and VPN scenarios. You can direct client traffic away from expensive and slow WAN links to instead use faster internet links to Microsoft Azure.

For more information, see CMG hierarchy design and Set up CMG.

Real-time management

Run CMPivot from the central administration site

Configuration Manager now supports running CMPivot from the central administration site in a hierarchy. The primary site still handles the communication to the client. When running CMPivot from the central administration site, it communicates with the primary site over the high-speed message subscription channel. This communication doesn't rely upon standard SQL replication between sites.

For more information, see CMPivot for real-time data.

Edit or copy PowerShell scripts

You can now **Edit** or **Copy** an existing PowerShell script used with the Run Scripts feature. Instead of recreating a script that you need to change, now directly edit it. Both actions use the same wizard experience as when you create a new script. When you edit or copy a script, Configuration Manager doesn't persist the approval state.

For more information, see Run Scripts.

Content management

Distribution point maintenance mode

You can now set a distribution point in maintenance mode. Enable maintenance mode when you're installing software updates, or making hardware changes to the server.

While the distribution point is in maintenance mode, it has the following behaviors:

- The site doesn't distribute any content to it.
- Management points don't return the location of this distribution point to clients.
- When you update the site, a distribution point in maintenance mode still updates.

- The distribution point properties are read-only. For example, you can't change the certificate or add boundary groups.
- Any scheduled task, like content validation, still runs on the same schedule.

For more information on this feature, see Maintenance mode.

For more information on automating this process with the Configuration Manager SDK, see SetDPMaintenanceMode method in class SMS_DistributionPointInfo.

Client management

Client provisioning mode timeout

The task sequence sets a timestamp when it puts the client in provisioning mode. A client in provisioning mode checks every 60 minutes the duration of time since the timestamp. If it's been in provisioning mode for more than 48 hours, the client automatically exits provisioning mode and restarts its process.

For more information, see Provisioning mode.

View first screen only during remote control

When connecting to a client with two or more monitors, it can be difficult to view them all in the Configuration Manager remote control viewer. A remote tools operator can now choose between seeing **All screens** or the **First screen** only.

For more information, see How to remotely administer a Windows client computer.

Specify a custom port for peer wakeup

You can now specify a custom port number for wake-up proxy. In client settings, in the **Power Management** group, configure the setting for **Wake On LAN port number (UDP)**.

For more information, see How to configure Wake on LAN.

Application management

Improvements to application approvals via email

This version has improvements to the feature to receive email notifications for application requests. Users could always add a comment to the request from Software Center. This comment shows on the application request in the Configuration Manager console. Now that comment also shows in the email. Including this comment in the email helps the approvers make a better decision to approve or deny the request.

For more information, see Email notifications.

Improvements to Package Conversion Manager

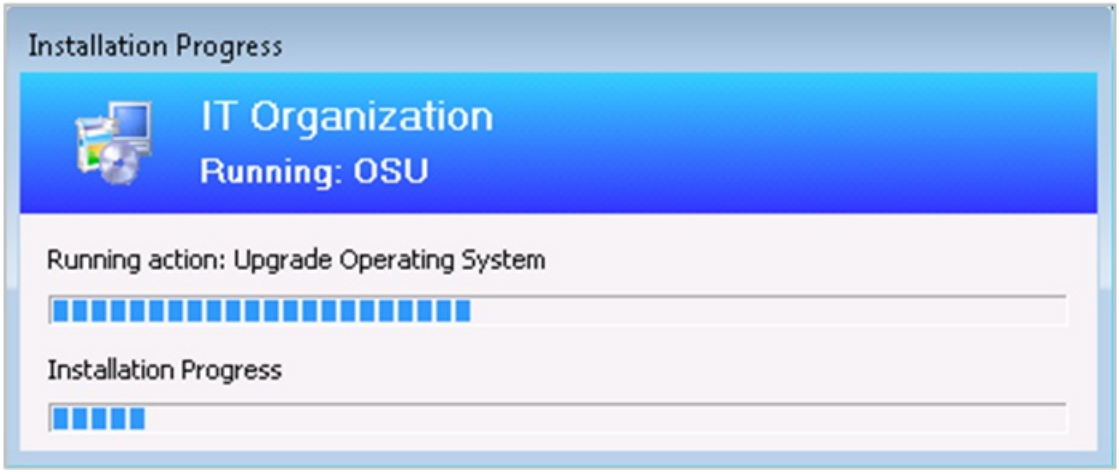
This version includes the following improvements to Package Conversion Manager:

- Scheduled package analysis runs every 7 days by default
- PowerShell cmdlets for analyzing and converting packages
- General bug fixes and improvements

OS deployment

Progress status during in-place upgrade task sequence

You now see a more detailed progress bar during a Windows 10 in-place upgrade task sequence. This bar shows the progress of Windows setup, which is otherwise silent during the task sequence. Users now have some visibility into the underlying progress. It helps with concerns that the upgrade process is suspended because of a lack of progress indication.



This feature works with any supported version of Windows 10, and only with the in-place upgrade task sequence.

Improvements to task sequence media creation

This version includes several improvements to help you better create and manage task sequence media. For more information, see the following articles for specific media types:

- Create stand-alone media
- Create prestaged media
- Create bootable media
- Create capture media

Specify temporary storage

When you create task sequence media, now customize the location that the site uses for temporary storage of data. This process can require a lot of temporary drive space. This change gives you greater flexibility to choose where to store these temporary files.

In the **Create Task Sequence Media Wizard**, specify a location for the **Staging folder**. By default this location is similar to the following path: `%UserProfile%\AppData\Local\Temp`.

Add a label to the media

You can now add a label to task sequence media. This label helps you better identify the media after you create it. In the **Create Task Sequence Media Wizard**, specify a **Media label**.

Include autorun.inf file on media

when you create task sequence media, Configuration Manager doesn't add an autorun.inf file. This file is commonly blocked by antimalware products. You can still include the file if necessary for your scenario.

Import a single index of an OS image

When importing a Windows image (WIM) file to Configuration Manager, you can now specify to automatically import a single index rather than all image indexes in the file. This option provides the following benefits:

- Smaller image file
- Faster offline servicing
- Optimize image servicing, for a smaller image file after offline servicing

When you import an OS image, select the option to **Extract a specific image index from the specified WIM file**. Then select the image index from the list.

For more information, see Add an OS image.

Optimized image servicing

When you apply software updates to an OS image, there's a new option to optimize the output by removing any superseded updates. The optimization to offline servicing only applies to images with a single index.

When you create a schedule to update an OS image, select the option to **Remove superseded updates after the image is updated**.

For more information, see Apply software updates to an image.

Improvements to Run PowerShell Script task sequence step

The **Run PowerShell Script** task sequence step now includes the following improvements:

- You can now directly enter Windows PowerShell code in this step. This change lets you run PowerShell commands during a task sequence without first creating and distributing a package with the script.
- When you choose the **Enter a PowerShell script** option, select **Edit Script**. The new PowerShell script window provides the following actions:
  - Edit the script directly
  - Open an existing script from file
  - Browse to an existing approved script in Configuration Manager
- Save the script output to a custom task sequence variable
- To include the script parameters in the task sequence log, set the task sequence variable **OSDLogPowerShellParameters** to **TRUE**. By default, the parameters aren't in the log.
- Other improvements that provide similar functionality as the Run Command Line step. For example, specify alternate user credentials or specify a time-out.

> **IMPORTANT**
> To take advantage of this new Configuration Manager feature, after you update the site, also update clients to the latest version. While new functionality appears in the Configuration Manager console when you update the site and console, the complete scenario isn't functional until the client version is also the latest.

For more information, see Run PowerShell Script.

Other improvements to OS deployment

This version includes the following improvements to OS deployment:

- There's a new **View** default action on task sequences.
- The task sequence error dialog window now displays more information. It shows the name of the task sequence step that failed.
- When you set the **OSDDoNotLogCommand** task sequence variable to true, now it also hides the command line from the Run Command Line step in the log file. It previously only masked the program name from the Install Package step in smsts.log.
- When you enable a PXE responder on a distribution point without Windows Deployment Service, it can now be on the same server as the DHCP service. For more information, see Configure at least one distribution point to accept PXE requests.

Software Center

Replace toast notifications with dialog window

Sometimes users don't see the Windows toast notification about a restart or required deployment. Then they don't see the experience to snooze the reminder. This behavior can lead to a poor user experience when the client reaches a deadline.

Now when deployments need a restart or software changes are required, you have the option of using a more intrusive dialog window.

For more information, see Plan for Software Center

Configure user device affinity in Software Center

With Software Center infrastructure improvements starting in version 1806, the application catalog site server roles are no longer required for most scenarios. Some customers still relied upon the application catalog to allow users to set their primary device for user device affinity.

Now users can set their primary device in Software Center. This action makes them a primary user of the device in Configuration Manager.

For more information, see Link users and devices with user device affinity.

Configure default views in Software Center

This version of Configuration Manager further iterates on how you can customize Software Center:

- Set the default layout of applications, either as tiles or a list
  - If a user changes this configuration, Software Center persists the user's preference in the future
- Configure the default application filter, either all or only required apps
  - Software Center always uses your default setting. Users can change this filter, but Software Center doesn't persist their preference.

Specify these settings in the **Software Center** group of client settings.

For more information, see About client settings.

Software updates

Specify priority for feature updates in Windows 10 servicing

Adjust the priority with which clients install a feature update through Windows 10 servicing. By default, clients now install feature updates with higher processing priority.

Use client settings to configure this option. In the **Software Updates** group, configure the following setting: **Specify thread priority for feature updates**.

For more information, see About client settings.

Office management

Redirect Windows known folders to OneDrive

Use Configuration Manager to move Windows known folders to OneDrive for Business. These folders include Desktop, Documents, and Pictures. To simplify your Windows 10 upgrades, deploy these settings to Windows 7 clients before deploying a task sequence.

For more information on this feature of OneDrive for Business, see Redirect and move Windows known folders to OneDrive.

First, find your Office 365 tenant ID. Then deploy the OneDrive sync client version 18.111.0603.0004 or later. For more information, see Deploy OneDrive apps by using System Center Configuration Manager.

To create and deploy a OneDrive for Business profile, in the Configuration Manager console, go to the **Assets and Compliance** workspace. Expand **Compliance Settings**, and select the **OneDrive for Business Profiles** node.

For more information, see the Redirect Windows known folders to OneDrive section in the OneDrive for Business

Profiles article.

Integration for Office 365 ProPlus readiness

Use Configuration Manager to identify devices with high confidence that are ready to upgrade to Office 365 ProPlus. The integration provides insights into any potential compatibility issues with Office add-ins and macros used in your environment. Then use Configuration Manager to deploy Office to ready devices.

The existing Office 365 client management dashboard now includes a new tile, **Office 365 ProPlus Upgrade Readiness**.

For more information, see Office 365 client management dashboard

Additional languages for Office 365 updates

Configuration Manager now supports all supported languages for Office 365 client updates. The update workflow now separates the 38 languages for **Windows Update** from the numerous languages for **Office 365 Client Update**.

For more information, see Manage Office 365 updates

Office products on lifecycle dashboard

The product lifecycle dashboard now includes information for installed versions of Office 2003 through Office 2016. Data shows up after the site runs the lifecycle summarization task, which is every 24 hours.

For more information, see Use the Product Lifecycle dashboard.

Phased deployments

Dedicated monitoring for phased deployments

Phased deployments now have their own dedicated monitoring node. This node makes it easier to identify phased deployments that you created and then navigate to the phased deployment monitoring view. In the Configuration Manager console, go to the **Monitoring** workspace, and select the **Phased Deployments** node. It shows the list of phased deployments.

For more information, see Phased deployment monitoring view.

Improvement to phased deployment success criteria

Specify additional criteria for the success of a phase in a phased deployment. Instead of only a percentage, this criteria can now also be the number of devices successfully deployed. This option is useful when the size of the collection is variable, and you have a specific number of devices to show success before moving to the next phase.

Create a phased deployment for a task sequence, software update, or application. Then on the Settings page of the wizard, select the following option as the criteria for success of the first phase: **Number of devices successfully deployed**.

For more information, see Create phased deployments.

Configuration Manager console

Improvements to Configuration Manager console

Based on customer feedback at the Midwest Management Summit (MMS) Desert Edition 2018, this version includes the following improvements to the Configuration Manager console:

- Maximize the browse registry window for application detection methods
- Go to the collection from an application deployment
- Remove content from monitoring status
- Views sort by integer values in the **Deployments** node of the **Monitoring** workspace

- Move the warning for a large number of results

For more information, see Using the Configuration Manager console.

Configuration Manager console notifications

To keep you better informed so that you can take the appropriate action, the Configuration Manager console now notifies you for the following events:

- When an update is available for Configuration Manager itself
- When lifecycle and maintenance events occur in the environment

This notification is a bar at the top of the console window below the ribbon. It replaces the previous experience when Configuration Manager updates are available. These in-console notifications still display critical information, but don't interfere with your work in the console. You can't dismiss critical notifications. The console displays all notifications in a new notification area of the title bar.

For more information, see Using the Configuration Manager console.

Confirmation of console feedback

When you send feedback in the Configuration Manager console, it now shows a confirmation message. This message includes a **Feedback ID**, which you can give to Microsoft as a tracking identifier.

For more information, see Product feedback.

View recently connected consoles

You can now view the most recent connections for the Configuration Manager console. The view includes active connections and those consoles that recently connected. In the Configuration Manager console, go to the **Administration** workspace, expand **Security**, and select the **Console Connections** node.

For more information, see Using the Configuration Manager console.

In-console documentation dashboard

There's a new **Documentation** node in the new **Community** workspace. This node includes up-to-date information about Configuration Manager documentation and support articles.

For more information, see Using the Configuration Manager console.

Search device views using MAC address

You can now search for a MAC address in a device view of the Configuration Manager console. This property is useful for OS deployment administrators while troubleshooting PXE-based deployments. When you view a list of devices, add the **MAC Address** column to the view. Use the search field to add the **MAC Address** search criteria.

For more information, see Using the Configuration Manager console.

Use .NET 4.7 for improved console accessibility

To improve the accessibility features of the Configuration Manager console, update .NET to version 4.7 or later on the computer running the console.

For more information, see Accessibility features in Configuration Manager.

Changes to console setup process

There are new components required when installing the Configuration Manager console. If you create a package for installing the console on other computers, make sure the package includes the following files:

- ConsoleSetup.exe
- AdminConsole.msi
- ConfigMgr.AC_Extension.i386.cab

- ConfigMgr.AC_Extension.amd64.cab

When you install or update a site server, it copies these installation files and supported language packs for the site to the **Tools\ConsoleSetup** subfolder. For more information, see Install the Configuration Manager console.

Other updates

Aside from new features, this release also includes additional changes such as bug fixes. For more information, see Summary of changes in Configuration Manager current branch, version 1902.

For more information on changes to the Windows PowerShell cmdlets for Configuration Manager, see PowerShell version 1902 release notes.

The following update rollup (4500571) is available in the console starting on 17 June 2019: Update rollup for Configuration Manager current branch, version 1902.

Next steps

When you're ready to install this version, see Installing updates for Configuration Manager and Checklist for installing update 1902.

> **TIP**
> To install a new site, use a baseline version of Configuration Manager.
>
> Learn more about:
>
> - Installing new sites
> - Baseline and update versions

For known, significant issues, see the Release notes.

After you update a site, also review the Post-update checklist.

What's new in version 1810 of Configuration Manager current branch

6/19/2019 • 15 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Update 1810 for Configuration Manager current branch is available as an in-console update. Apply this update on sites that run version 1710, 1802, or 1806. This article summarizes the changes and new features in Configuration Manager, version 1810.

Always review the latest checklist for installing this update. For more information, see Checklist for installing update 1810. After you update a site, also review the Post-update checklist.

To take advantage of new Configuration Manager features, first update clients to the latest version. While new functionality appears in the Configuration Manager console when you update the site and console, the complete scenario isn't functional until the client version is also the latest.

TIP

To get notified when this page is updated, copy and paste the following URL into your RSS feed reader:

```
https://docs.microsoft.com/api/search/rss?search=%22what%27s+new+in+version+1810+-
+Configuration+Manager%22&locale=en-us
```

Deprecated features and operating systems

Learn about support changes before they're implemented in removed and deprecated items.

Starting on August 14, 2018, the hybrid mobile device management feature is deprecated. For more information, see What is hybrid MDM.

Support for System Center Endpoint Protection (SCEP) for Mac and Linux (all versions) ends on December 31, 2018. Availability of new virus definitions for SCEP for Mac and SCEP for Linux may be discontinued after the end of support. For more information, see End of support blog post.

Classic service deployments in Azure are now deprecated in Configuration Manager. Start using Azure Resource Manager deployments for the cloud management gateway and the cloud distribution point. For more information, see Plan for CMG.

Site infrastructure

Support for Windows Server 2019

Configuration Manager now supports Windows Server 2019 and Windows Server, version 1809, as site systems.

For more information, see Supported operating systems for site system servers.

Hierarchy support for site server high availability

Central administration sites and child primary sites can now have an additional site server in passive mode.

For more information, see Site server high availability.

Improvements to setup prerequisites

When you install or update to version 1810, Configuration Manager setup now includes or improves the following

prerequisite checks:

- **Pending system restart**: This prerequisite check is now more resilient. It checks additional registry keys for Windows features. For more information, see Pending system restart.
- **SQL change tracking cleanup**: A new check if the site database has a backlog of SQL change tracking data. For more information, including a procedure to verify and clear this backlog, see SQL change tracking cleanup.
- **SQL Native Client version**: This prerequisite check is updated for versions of SQL Native Client that support TLS 1.2. The minimum version is SQL 2012 SP4. For more information, see SQL Native Client version.
- **Site system on Windows cluster node**: The Configuration Manager setup process no longer blocks installation of the site server role on a computer with the Windows role for Failover Clustering. SQL Always On requires this role, so previously you couldn't colocate the site database on the site server. With this change, you can create a highly available site with fewer servers by using SQL Always On and a site server in passive mode. For more information, see Windows Failover Cluster.

New permission for client notification actions

Client notification actions now require the **Notify Resource** permission on the SMS_Collection class. The following built-in roles have this permission by default:

- Full Administrator
- Infrastructure Administrator

Add this permission to any custom roles that need to use client notification actions.

For more information, see Client notifications.

Content management

New boundary group options

Boundary groups now include the following additional settings to give you more control over content distribution in your environment:

- **Prefer distribution points over peers with the same subnet**: By default, the management point prioritizes peer cache sources at the top of the list of content locations. This setting reverses that priority for clients that are in the same subnet as the peer cache source.
- **Prefer cloud distribution points over distribution points**: If you have a branch office with a faster internet link, you can now prioritize cloud content.

For more information, see Boundary group options for peer downloads.

Management insights rule for peer cache source client version

The **Management Insights** node has a new rule to identify clients that serve as a peer cache source but haven't upgraded from a pre-1806 client version. The new rule is **Upgrade peer cache sources to the latest version of the Configuration Manager client**, and is part of the new **Proactive Maintenance** rule group. Pre-1806 clients can't be used as a peer cache source for clients that run version 1806 or later. Select **Take action** to open a device view that displays the list of clients.

For more information, see Management insights.

Client management

New client notification action to wake up device

You can now wake up clients from the Configuration Manager console, even if the client isn't on the same subnet as the site server. If you need to do maintenance or query devices, you're not limited by remote clients that are asleep. The site server uses the client notification channel to identify another client that's awake on the same remote subnet. The awake client then sends a wake on LAN request (magic packet).

For more information, see Configure Wake on LAN and How to wake up clients.

New option to perform client notification from devices node

Up until 1810, the **Client Notification** option was only available from either the Device Collection node or when you viewed the membership of a Device Collection. It's now possible to perform a **Client Notification** from the **Devices** node directly. There's no longer a requirement to be within a collection membership view.

For more information, see Client notifications.

Improvements to collection evaluation

The following changes in collection evaluation behavior can improve site performance:

- Previously, when you configured a schedule on a query-based collection, the site would continue to evaluate the query whether or not you enabled the collection setting to **Schedule a full update on this collection**. To fully disable the schedule, you had to change the schedule to **None**. Now the site clears the schedule when you disable this setting. To specify a schedule for collection evaluation, enable the option to **Schedule a full update on this collection**.
- You can't disable the evaluation of built-in collections like **All Systems**, but now you can configure the schedule. This behavior allows you to customize this action at a time that meets your business requirements.

For more information, see How to create collections.

Improvement to client installation

When installing the Configuration Manager client, the ccmsetup process contacts the management point to locate the necessary content. Previously in this process the management point only returns distribution points in the client's current boundary group. If no content is available, the setup process falls back to download content from the management point. There's no option to fall back to distribution points in other boundary groups that might have the necessary content. Now the management point returns distribution points based on boundary group configuration.

For more information, see Configure boundary groups.

Co-management

Required app compliance policy for co-managed devices

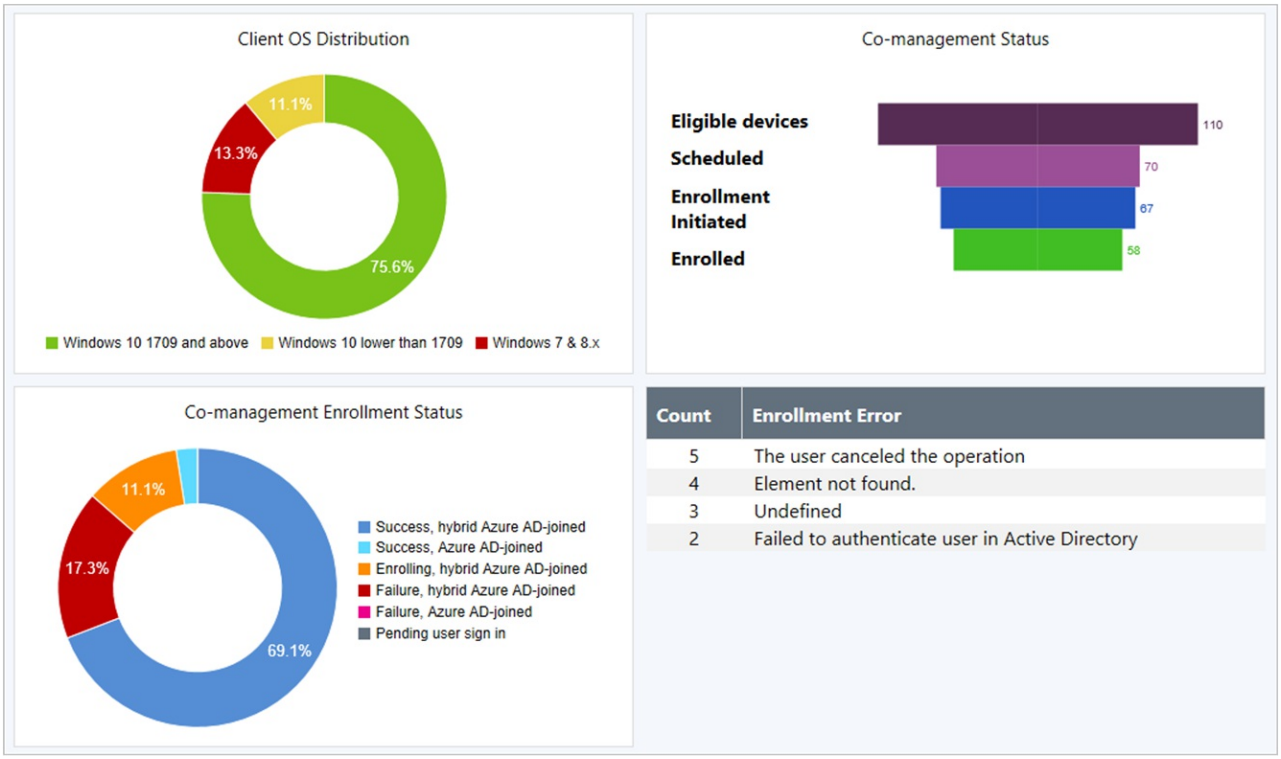
Define compliance policy rules in Configuration Manager for required applications. This app assessment is part of the overall compliance state sent to Microsoft Intune for co-managed devices.

For more information, see Co-management workloads.

Improvement to co-management dashboard

The co-management dashboard is enhanced with the following more detailed information:

- The **Co-management enrollment status** tile includes additional states
- A new **Co-management status** tile with a funnel chart shows states of the enrollment process
- A new tile with counts of **Enrollment errors**



For more information, see Co-management dashboard.

Improvements to internet-based client setup

This release further simplifies the Configuration Manager client setup process for clients on the internet. The site publishes additional Azure Active Directory (Azure AD) information to the cloud management gateway (CMG). An Azure AD-joined client gets this information from the CMG during the ccmsetup process, using the same tenant to which it's joined. This behavior further simplifies enrolling devices to co-management in an environment with more than one Azure AD tenant. Now the only two required ccmsetup properties are **CCMHOSTNAME** and **SMSSiteCode**.

For more information, see How to prepare internet-based devices for co-management.

Application management

Convert applications to MSIX

Starting in version 1806, Configuration Manager supports deployment of the new Windows 10 app package (.msix) format. Now you can convert your existing Windows Installer (.msi) applications to the MSIX format.

For more information, see Create Windows applications.

Repair applications

Specify a repair command line for Windows Installer and Script Installer deployment types. Then if you enable the option on the deployment, a new button is available in Software Center to **Repair** the application. When you configure an application with a repair program, users can start the command from Software Center.

For more information, see Create applications and Deploy applications.

Approve application requests via email

Configure email notifications for application approval requests. When a user requests an application, you receive an email. Click links in the email to approve or deny the request, without requiring the Configuration Manager console.

For more information, see Approve applications.

Detection methods don't load Windows PowerShell profiles

You can use Windows PowerShell scripts for detection methods on applications and settings in configuration items. When these scripts run on clients, the Configuration Manager client now calls PowerShell with the `-NoProfile` parameter. This option starts PowerShell without profiles.

A PowerShell profile is a script that runs when PowerShell starts. You can create a PowerShell profile to customize your environment and to add session-specific elements to every PowerShell session that you start.

> **NOTE**
> This change in behavior doesn't apply to Scripts or CMPivot. Both of these features already use this PowerShell parameter.

For more information, see Create applications and Create custom configuration items.

OS deployment

Task sequence support of Windows Autopilot for existing devices

Windows Autopilot for existing devices is now available with Windows 10, version 1809 or later. This new feature allows you to reimage and provision a Windows 7 device for Windows Autopilot user-driven mode using a single, native Configuration Manager task sequence.

For more information, see Windows Autopilot for existing devices.

Specify the drive for offline OS image servicing

Now specify the drive that Configuration Manager uses when adding software updates to OS images and OS upgrade packages. This process can consume a large amount of disk space with temporary files, so this option gives you flexibility to select the drive to use.

For more information, see Manage OS images or Manage OS upgrade packages.

Task sequence support for boundary groups

When a device runs a task sequence and needs to acquire content, it now uses boundary group behaviors similar to the Configuration Manager client.

For more information, see Boundary groups.

Improvements to driver maintenance

Driver packages now have additional metadata fields for **Manufacturer** and **Model**. Use these fields to tag driver packages with information to assist in general housekeeping, or to identify old and duplicate drivers that you can delete.

For more information, see Manage drivers.

Improvements to Windows 10 servicing plan filters

Additional filters have been added to Windows 10 servicing plans. You can now filter by **Architecture**, **Product Category**, and if the upgrade is **Superseded**.

For more information, see Windows 10 servicing plan.

New task sequence variable for last action name

Along with the task sequence variable _SMSTSLastActionRetCode, the task sequence also sets a new variable **_SMSTSLastActionName**. It also logs this value to the smsts.log file. This new variable is beneficial when troubleshooting a task sequence. When a step fails, a custom script can include the step name along with the return code.

For more information, see Task sequence variables.

Software updates

Phased deployment of software updates

Create phased deployments for software updates. Phased deployments allow you to orchestrate a coordinated, sequenced rollout of software based on customizable criteria and groups.

For more information, see Create phased deployments.

Improvement to maintenance windows for software updates

The following client setting is in the **Software Updates** group to control the installation behavior of software updates in maintenance windows: **Enable installation of updates in "All deployments" maintenance window when "Software update" maintenance window is available**

By default, this option is **No** to keep consistent with the existing behavior. Change it to **Yes** to allow clients to use other available maintenance windows to install software updates.

For more information, see Software updates client settings.

Improvement to software updates maintenance

WSUS cleanup tasks now run on secondary sites. WSUS cleanup for expired updates is run and superseded updates are declined in WSUS for secondary sites.

For more information, see WSUS cleanup behavior starting in version 1810

Improvement to software update supersedence rules

You can now specify supersedence rules for feature updates separately from non-feature updates. This means your upgrades won't be removed from Configuration Manager before you have completed servicing your Windows 10 clients.

For more information, see Supersedence rules.

Reporting

Improvement to lifecycle dashboard

The product lifecycle dashboard now includes information for **System Center 2012 Configuration Manager and later**.

There's also a new report, **Lifecycle 05A - Product lifecycle dashboard**. It includes similar information as the in-console dashboard.

For more information on this dashboard, see Use the Product Lifecycle dashboard.

Improvement to data warehouse

You can now synchronize more tables from the site database to the data warehouse. This change allows you to create more reports based on your business requirements.

For more information, see Data warehouse.

Configuration Manager console

Configuration Manager administrator authentication

You can now specify the minimum authentication level for administrators to access Configuration Manager sites. This feature enforces administrators to sign in to Windows with the required level. To configure this setting, find the **Authentication** tab in **Hierarchy Settings**.

For more information, see Plan for the SMS Provider.

Support Center

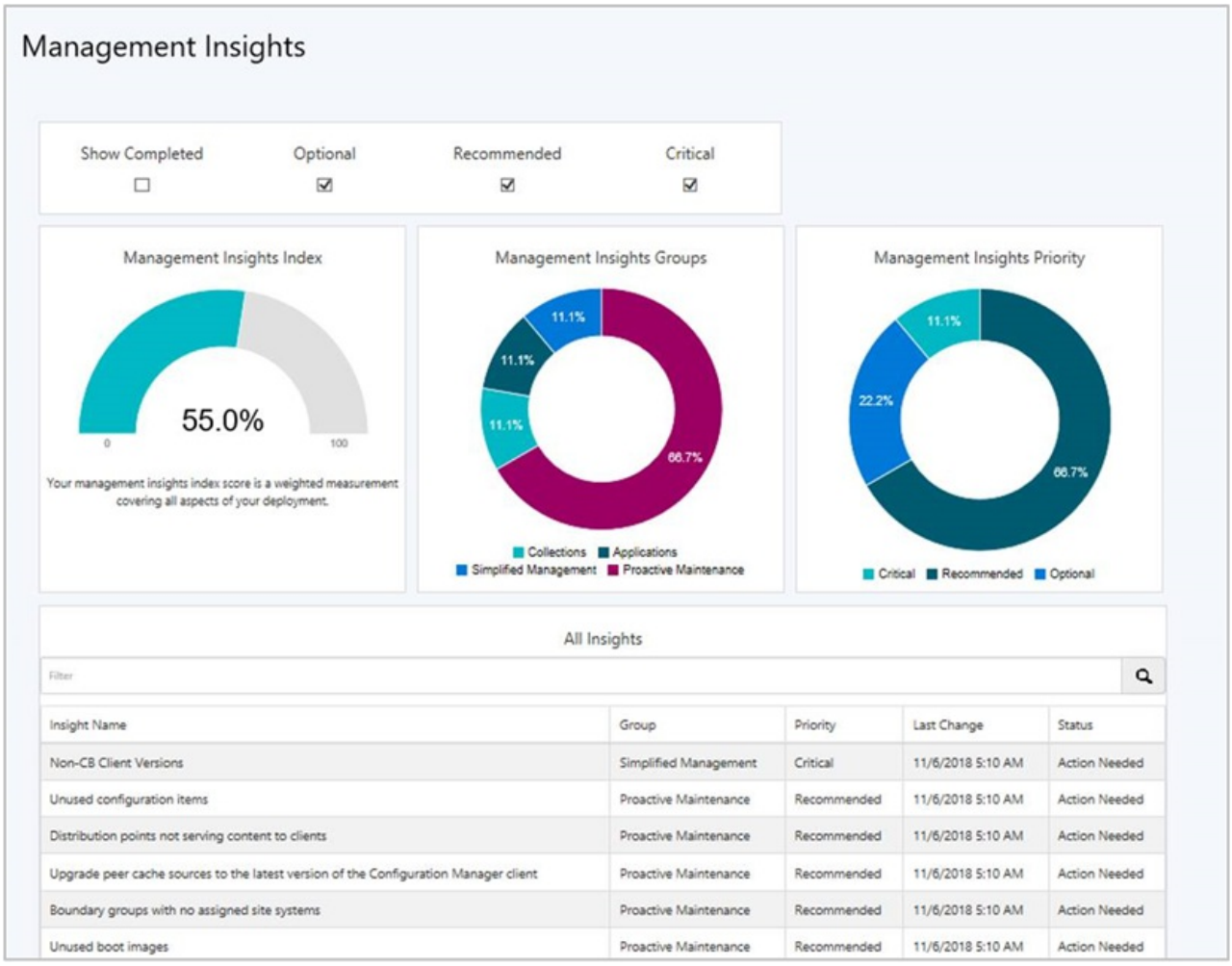
Use Support Center for client troubleshooting, real-time log viewing, or capturing the state of a Configuration Manager client computer for later analysis. Support Center is a single tool to combine many administrator troubleshooting tools. Find the Support Center installer on the site server in the **cd.latest\SMSSETUP\Tools\SupportCenter** folder.

For more information, see Support Center.

Management insights dashboard

The **Management Insights** node now includes a graphical dashboard. This dashboard displays an overview of the rule states, which makes it easier for you to show your progress. The dashboard includes the following tiles:

- **Management insights index**: Tracks overall progress on management insights rules. The index is a weighted average. Critical rules are worth the most. This index gives the least weight to optional rules.
- **Management insights groups**: Shows percent of rules in each group.
- **Management insights priority**: Shows percent of rules by priority.
- **All insights**: A table of insights including priority and state.



For more information, see Management insights.

Improvements to CMPivot

CMPivot includes the following improvements:

- Save **Favorite** queries
- On the Query Summary tab, select the count of Failed or Offline devices, and then select the option to **Create Collection**.

For more information on additional performance and troubleshooting improvements to CMPivot, see Improvements to scripts.

For more information on CMPivot, see CMPivot.

Improvements to scripts

You can now view detailed script output in raw or structured JSON format. This formatting makes the output easier to read and analyze.

The following performance and troubleshooting improvements apply to both CMPivot and scripts:

- Updated clients return output less than 80 KB to the site over a fast communication channel. This change increases the performance of viewing script or query output.
- Additional logs for troubleshooting

For more information, see the following articles:

- Create and run PowerShell scripts from the Configuration Manager console
- Troubleshooting CMPivot

SMS Provider API

The SMS Provider now provides read-only API interoperability access to WMI over HTTPS, called the **administration service**. This REST API can be used in place of a custom web service to access information from the site.

The **SMS Provider** appears as a role with an option to allow communication over the cloud management gateway. The current use for this setting is to enable application approvals via email from a remote device.

For more information, see Plan for the SMS Provider.

On-premises MDM

An Intune connection is no longer required for new on-premises MDM deployments

The on-premises MDM prerequisite to configure a Microsoft Intune subscription is no longer required for new deployments. Your organization still requires Intune licenses to use this feature. You can't currently remove the Intune connection from existing on-premises MDM deployments. For more information, see the Intune support blog post.

Other updates

Aside from new features, this release also includes additional changes such as bug fixes. For more information, see Summary of changes in Configuration Manager current branch, version 1810.

For more information on changes to the Windows PowerShell cmdlets for Configuration Manager, see PowerShell version 1810 release notes.

The following update rollup (4488598) is available in the console starting on 25 March 2019: Update rollup 2 for Configuration Manager current branch, version 1810. This replaces the prior update rollup, KB 4486457.

Hotfixes

The following additional hotfixes are available to address specific issues:

ID	TITLE	DATE	IN-CONSOLE

ID	TITLE	DATE	IN-CONSOLE
4487960	Microsoft Intune connector certificate does not renew in Configuration Manager	18 January 2019	Yes
4490434	Duplicate user discovery columns are created in Configuration Manager	22 February 2019	Yes
4490575	Update installations stop responding or never show completion in Configuration Manager, version 1810	22 February 2019	Yes

Next steps

When you're ready to install this version, see Installing updates for Configuration Manager and Checklist for installing update 1810.

> **TIP**
> To install a new site, use a baseline version of Configuration Manager.
>
> Learn more about:
>
> - Installing new sites
> - Baseline and update versions

For known, significant issues, see the Release notes.

After you update a site, also review the Post-update checklist.

What's new in version 1806 of Configuration Manager current branch

8/28/2019 • 23 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Update 1806 for Configuration Manager current branch is available as an in-console update. Apply this update on sites that run version 1706, 1710, or 1802.

Always review the latest checklist for installing this update. For more information, see Checklist for installing update 1806. After you update a site, also review the Post-update checklist.

The following sections provide details about the changes and new features in version 1806 of Configuration Manager current branch.

Deprecated features and operating systems

Learn about support changes before they are implemented in removed and deprecated items.

As of August 14, 2018, the hybrid mobile device management feature is deprecated. For more information, see What is hybrid MDM.

Site infrastructure

CMPivot

Configuration Manager has always provided a large centralized store of device data, which customers use for reporting purposes. The site typically collects this data on a weekly basis. CMPivot is a new in-console utility that now provides access to real-time state of devices in your environment. It immediately runs a query on all currently connected devices in the target collection and returns the results. You can then filter and group this data in the tool. By providing real-time data from online clients, you can more quickly answer business questions, troubleshoot issues, and respond to security incidents.

For more information, see CMPivot.

Site server high availability

High availability for a standalone primary site server role is a Configuration Manager-based solution to install an additional site server in passive mode. The site server in passive mode is in addition to your existing site server that is in active mode. A site server in passive mode is available for immediate use, when needed.

For more information, see the following articles:

- Site server high availability
- Flowchart - Set up a site server in passive mode
- Flowchart - Promote site server (planned)
- Flowchart - Promote site server (unplanned)

Improvements to management insights

This release includes the following improvements to management insights:

- Some management insights now have the option to take an action. This action is either navigating to the associated node in the console, or showing a filtered, query-based view.

- A new group for Proactive Maintenance is available with six new rules, which help highlight potential configuration issues to avoid through regular upkeep.

For more information, see Management insights.

Configuration Manager tools

The Configuration Manager server and client tools are now included on the server. Find them in the `CD.Latest\SMSSETUP\Tools` folder on the site server. No further installation required.

For more information, see Configuration Manager tools.

Exclude Active Directory containers from discovery

To reduce the number of discovered objects, exclude specific containers from Active Directory system discovery.

For more information, see Configure Active Directory System Discovery.

Content management

Configure a remote content library for the site server

To configure site server high availability or to free up hard drive space on your central administration or primary site servers, relocate the content library to another storage location. Move the content library to another drive on the site server, a separate server, or fault-tolerant disks in a storage area network (SAN).

For more information, see the following articles:

- The content library
- Flowchart - Manage content library

Cloud distribution point support for Azure Resource Manager

When creating a cloud distribution point, the wizard now provides the option to create an **Azure Resource Manager deployment**. Azure Resource Manager is a modern platform for managing all solution resources as a single entity, called a resource group. When deploying a cloud distribution point with Azure Resource Manager, the site uses Azure Active Directory to authenticate and create the necessary cloud resources. This modernized deployment doesn't require the classic Azure management certificate.

The feature documentation for the cloud distribution point is also revised and enhanced. For more information, see the following articles:

- Use a cloud distribution point
- Install a cloud distribution point

Pull-distribution points support cloud distribution points as source

Many customers use pull-distribution points in remote or branch offices, which download content from a source distribution point across the WAN. If your remote offices have a better connection to the internet, or to reduce load on your WAN links, you can now use a cloud distribution point in Microsoft Azure as the source. When you add a source on the **Pull Distribution Point** tab of the distribution point properties, any cloud distribution point in the site is now listed as an available distribution point. The behavior of both site system roles remains the same otherwise.

For more information, see Use a pull-distribution points.

Enable distribution points to use network congestion control

Windows Low Extra Delay Background Transport (LEDBAT) is a feature of Windows Server to help manage background network transfers. For distribution points running on supported versions of Windows Server, enable an option to help adjust network traffic. Clients only use network bandwidth when it's available.

For more information, see Windows LEDBAT.

Partial download support in client peer cache to reduce WAN utilization

Client peer cache sources can now divide content into parts. These parts minimize the network transfer to reduce WAN utilization. The management point provides more detailed tracking of the content parts. It tries to eliminate more than one download of the same content per boundary group.

For more information, see Partial download support.

Boundary group options for peer downloads

Boundary groups now include additional settings to give you more control over content distribution in your environment. This release adds the following options:

- **Allow peer downloads in this boundary group**: The management point provides clients a list of content locations that includes peer sources. This setting also affects applying Group IDs for Delivery Optimization.
- **During peer downloads, only use peers within the same subnet**: The management point only includes in the content location list peer sources that are in the same subnet as the client.

For more information, see Boundary group options for peer downloads.

Improvement to peer cache source location status

Configuration Manager is more efficient at determining if a peer cache source has roamed to another location. This behavior makes sure the management point offers it as a content source to clients in the new location and not the old location. If you're using the peer cache feature with roaming peer cache sources, after updating the site to version 1806, also update all peer cache sources to the latest client version. The management point doesn't include these peer cache sources in the list of content locations until they are updated to at least version 1806.

For more information, see Requirements for peer cache.

Client management

Improvement to client push security

When using the client push method of installing the Configuration Manager client, the site can now require Kerberos mutual authentication. This enhancement helps to secure the communication between the server and the client.

For more information, see How to install clients with client push.

Enhanced HTTP site system

Using HTTPS communication is recommended for all Configuration Manager communication paths, but can be challenging for some customers due to the overhead of managing PKI certificates.

This release includes improvements to how clients communicate with site systems. On the site properties, **Client Computer Communication** tab, select the option for **HTTPS or HTTP**, and then enable the new option to **Use Configuration Manager-generated certificates for HTTP site systems**. This feature is a pre-release feature.

For more information, see Enhanced HTTP.

Azure AD device identity

An Azure AD-joined or hybrid Azure AD device without an Azure AD user signed in can securely communicate with its assigned site. The cloud-based device identity is now sufficient to authenticate with the CMG and management point.

For more information, see Enhanced HTTP.

CMTrace installed with client

The CMTrace log viewing tool is now automatically installed along with the Configuration Manager client. It's added to the client installation directory, which by default is `%WinDir%\ccm\cmtrace.exe`.

For more information, see CMTrace.

Cloud management dashboard

The new cloud management dashboard provides a centralized view for cloud management gateway (CMG) usage. When the site is onboarded with Azure AD, it also displays data about cloud users and devices.

This feature also includes the **CMG connection analyzer** for real-time verification to aid troubleshooting. The in-console utility checks the current status of the service, and the communication channel through the CMG connection point to any management points that allow CMG traffic.

For more information, see the following sections of the Monitor CMG article:

- Cloud management dashboard
- Connection analyzer

Improvements to cloud management gateway

Version 1806 includes the following improvements to the cloud management gateway (CMG):

Simplified client bootstrap command line

When installing the Configuration Manager client on the internet via a CMG, the command-line now requires fewer properties. This improvement reduces the size of the command line used in Microsoft Intune when preparing for co-management.

For more information, see How to prepare internet-based devices for co-management.

Download content from a CMG

Previously, you had to deploy a cloud distribution point and CMG as separate roles. A CMG can now also serve content to clients. This functionality reduces the required certificates and cost of Azure VMs.

For more information, see Modify a CMG.

Trusted root certificate isn't required with Azure AD

When you create a CMG, you're no longer required to provide a trusted root certificate on the Settings page. This certificate isn't required when using Azure Active Directory (Azure AD) for client authentication, but used to be required in the wizard. If you're using PKI client authentication certificates, then you still must add a trusted root certificate to the CMG.

Co-management

Sync MDM policy from Microsoft Intune for a co-managed device

When you switch a co-management workload, the co-managed devices automatically synchronize MDM policy from Microsoft Intune. This sync also happens when you initiate the **Download Computer Policy** action from Client Notifications in the Configuration Manager console.

For more information, see How to switch Configuration Manager workloads to Intune.

Transition new workloads to Intune using co-management

The following workloads are now able to transition from Configuration Manager to Intune after enabling co-management:

- **Device configuration**: This workload lets you use Intune to deploy MDM policies, while continuing to use Configuration Manager for deploying applications.
- **Office 365**: Devices don't install Office 365 deployments from Configuration Manager.
- **Mobile apps**: Any available apps deployed from Intune are available in the Company Portal. Apps that you deploy from Configuration Manager are available in Software Center. This feature is a pre-release feature.

To transition these workloads, go to the co-management properties page and move the workload slider bar from Configuration Manager to **Pilot** or **All**.

For more information, see Co-management for Windows 10 devices.

Support for multiple hierarchies to one Intune tenant

Some customers have several Configuration Manager hierarchies and want to consolidate in the future to a single tenant for Azure Active Directory and Microsoft Intune. Co-management now supports connecting more than one Configuration Manager environment to the same Intune tenant.

For more information, see Co-management prerequisites.

Compliance settings

Configure Windows Defender SmartScreen settings for Microsoft Edge

The Microsoft Edge browser compliance settings policy adds the following three settings for Windows Defender SmartScreen:

- Allow SmartScreen
- Users can override SmartScreen prompt for sites
- Users can override SmartScreen prompt for files

For more information, see Configure Microsoft Edge settings.

SCAP extensions

Convert Security Content Automation Protocol (SCAP) content to compliance settings baselines and generate SCAP reports using a console extension. This feature also includes a new dashboard to visualize the client compliance as well as XCCDF rule compliance.

For more information, see About the SCAP extensions.

Application management

Phased deployment of applications

Create a phased deployment for an application. Phased deployments allow you to orchestrate a coordinated, sequenced rollout of software based on customizable criteria and groups. For example, deploy the application to a pilot collection, and then automatically continue the rollout based on success criteria.

For more information, see the following articles:

- Create a phased deployment
- Manage and monitor phased deployments

Provision Windows app packages for all users on a device

Provision an application with a Windows app package for all users on the device. One common example of this scenario is provisioning an app from the Microsoft Store for Business and Education, like Minecraft: Education Edition, to all devices used by students in a school. Previously, Configuration Manager only supported installing these applications per user. After signing in to a new device, a student would have to wait to access an app. Now when the app is provisioned to the device for all users, they can be productive more quickly.

For more information, see Create Windows applications.

Office Customization Tool integration with the Office 365 Installer

The Office Customization Tool is now integrated with the Office 365 Installer in the Configuration Manager console. When creating a deployment for Office 365, dynamically configure the latest Office manageability

settings. Microsoft updates the Office Customization Tool when they release new builds of Office 365. This integration allows you to take advantage of new manageability settings in Office 365 as soon as they're available.

For more information, see Deploy Office 365 apps.

Support for new Windows app package formats

Configuration Manager now supports the deployment of new Windows 10 app package (.msix) and app bundle (.msixbundle) formats.

For more information, see Create Windows applications.

Uninstall application on approval revocation

The behavior has changed when you revoke approval for an application. Now when you deny the request for the application, the client uninstalls the application from the user's device. This behavior requires that you enable the optional feature **Approve application requests for users per device**.

For more information, see Deploy applications.

Package Conversion Manager

Package Conversion Manager is now an integrated tool that allows you to convert legacy packages into Configuration Manager current branch applications. Then you can use features of applications such as dependencies, requirement rules, and user device affinity.

For more information, see Package Conversion Manager.

OS deployment

Improvements to phased deployments

This release includes the following improvements to phased deployments:

Create a phased deployment with manually configured phases

For a task sequence, now manually configure the phases when you create a phased deployment. Add up to 10 additional phases from the **Phases** tab of the Create Phased Deployment wizard. You can still automatically create a default two-phase deployment.

For more information, see Create a phased deployment with manually configured phases.

Phased deployment status

Phased deployments now have a native monitoring experience. From the **Deployments** node in the **Monitoring** workspace, select a phased deployment, and then click **Phased Deployment Status** in the ribbon.

For more information, see Manage and monitor phased deployments.

Gradual rollout during phased deployments

During a phased deployment, the rollout in each phase can now happen gradually. This behavior helps mitigate the risk of deployment issues, and decreases the load on the network caused by the distribution of content to clients. The site can gradually make the software available depending on the configuration for each phase. Every client in a phase has a deadline relative to the time the software is made available. The time window between the available time and deadline is the same for all clients in a phase.

For more information, see Phase settings.

Improvements to Windows 10 in-place upgrade task sequence

The default task sequence template for Windows 10 in-place upgrade now includes another new group with recommended actions to add in case the upgrade process fails. These actions make it easier to troubleshoot. One such tool is Windows SetupDiag. It's a standalone diagnostic tool to obtain details about why a Windows 10 upgrade was unsuccessful.

For more information, see Create a task sequence to upgrade an OS.

Improvements to PXE-enabled distribution points

On the **PXE** tab of the distribution point properties, check **Enable a PXE responder without Windows Deployment Service**. This new option enables a PXE responder on the distribution point, which doesn't require Windows Deployment Services (WDS). Because WDS isn't required, the PXE-enabled distribution point can be a client or server OS, including Windows Server Core. This new PXE responder service supports IPv6, and also enhances the flexibility of PXE-enabled distribution points in remote offices.

For more information, see enable PXE on the distribution point.

Network access account not required for some scenarios

The Enhanced HTTP site system feature also removes some dependencies on the network access account. When you enable the new site option to **Use Configuration Manager-generated certificates for HTTP site systems**, the following scenarios don't require a network access account to download content from a distribution point:

- Task sequences running from boot media or PXE
- Task sequences running from Software Center

These task sequences can be for OS deployment or custom. It's also supported for workgroup computers.

For more information, see Task sequences and the network access account.

Other improvements to OS deployment

Mask sensitive data stored in task sequence variables

In the **Set Task Sequence Variable** step, select the new option to **Do not display this value**.

For more information, see Set Task Sequence Variable.

Mask program name during Run Command Step of a task sequence

To prevent potentially sensitive data from being displayed or logged, configure the task sequence variable **OSDDoNotLogCommand**.

For more information, see Task sequence variables.

Task sequence variable for DISM parameters when installing drivers

To specify additional command-line parameters for DISM, use the new task sequence variable **OSDInstallDriversAdditionalOptions**.

For more information, see Task sequence variables.

Option to use full disk encryption

Both the **Enable BitLocker** and **Pre-provision BitLocker** steps now include an option to **Use full disk encryption**. By default, these steps encrypt used space on the drive. This default behavior is recommended, as it's faster and more efficient.

For more information see Enable BitLocker and Pre-provision BitLocker.

Client provisioning mode isn't enabled with Windows 10 upgrade compatibility scan

Now when you enable the option to **Perform Windows Setup compatibility scan without starting upgrade**, the **Upgrade Operating System** task sequence step doesn't put the Configuration Manager client into provisioning mode.

For more information, see Upgrade Operating System.

Revised documentation for task sequence variables

Two new articles are now available for understanding task sequence variables:

- How to use task sequence variables is a new article that describes the different types of variables, methods to set the variables, and how to access them.

- Task sequence variables is a reference for all available task sequence variables. This article combines the previous articles, which separated built-in variables from action variables.

Software Center

> **IMPORTANT**
> To take advantage of new Configuration Manager features, first update clients to the latest version. While new functionality appears in the Configuration Manager console when you update the site and console, the complete scenario isn't functional until the client version is also the latest.

Software Center infrastructure improvements

Application catalog roles are no longer required to display user-available applications in Software Center. This change helps you reduce the server infrastructure required to deliver applications to users. Software Center now relies upon the management point to obtain this information, which helps larger environments scale better by assigning them to boundary groups.

For more information, see Configure Software Center

> **NOTE**
> The application catalog website point and web service point roles are no longer *required* in 1806, but still *supported* roles.
>
> The **Silverlight user experience** for the application catalog website point is no longer supported. For more information, see Removed and deprecated features.

Specify the visibility of the application catalog website link in Software Center

Use client settings to control whether the link to **Open the Application Catalog web site** appears in the **Installation status** node of Software Center.

For more information, see Software Center client settings.

> **NOTE**
> The **Silverlight user experience** for the application catalog website point is no longer supported. For more information, see Removed and deprecated features.

Custom tab for webpage in Software Center

Use client settings to create a customized tab to open a webpage in Software Center. This feature allows you to show content to your end users in a consistent, reliable way. The following list includes a few examples:

- Contact IT: information on how to contact your organization's IT department
- IT Support Center: IT self-service actions such as searching a knowledge base or opening a support ticket.
- End-user documentation: articles for users in your organization on various IT topics such as using applications or upgrading to Windows 10.

For more information, see Software Center client settings and the Software Center user guide.

Maintenance windows in Software Center

Software Center now displays the next scheduled maintenance window. On the Installation Status tab, switch the view from All to Upcoming. It displays the time range and the list of deployments that are scheduled. If there are no future maintenance windows, the list is blank.

For more information, see How to use maintenance windows and the Software Center user guide.

Software updates

Third-party software updates

Third-party software updates allow you to subscribe to partner catalogs in the Configuration Manager console and publish the updates to WSUS. You can then deploy these updates using the existing software update management process.

For more information, see Enable third-party updates.

Deploy software updates without content

Deploy software updates to devices without first downloading and distributing content to distribution points. This feature is beneficial when dealing with extremely large update content, or when you always want clients to get content from the Microsoft Update cloud service. Clients in this scenario can also download content from peers that already have the necessary content. The Configuration Manager client continues to manage the content download, thus can utilize the Configuration Manager peer cache feature, or other technologies such as Delivery Optimization. This feature supports any update type supported by Configuration Manager software updates management, including Windows and Office updates.

For more information, see the **No deployment package** option when you Manually deploy software updates or Automatically deploy software updates.

Filter automatic deployment rules by software update architecture

You can now filter automatic deployment rules (ADR) to exclude architectures like Itanium and ARM64. On the **Software Updates** page of the Create Automatic Deployment Rule Wizard, the **Architecture** property filter is now available.

For more information, see Automatically deploy software updates.

Improved WSUS maintenance

The WSUS cleanup wizard now declines updates that are expired according to the supersedence rules defined on the software update point component properties.

For more information, see Software updates maintenance.

Reporting

New software updates compliance report

Viewing reports for software updates compliance traditionally includes data from clients that haven't recently contacted the site. A new report, **Compliance 9 - Overall health and compliance**, lets you filter compliance results for a specific software update group by "healthy" clients. This report shows the more realistic compliance state of the active clients in your environment.

For more information, see Software updates reports.

Inventory

Improvement to hardware inventory for large integer values

Hardware inventory previously had a limit for integers larger than 4,294,967,296 (2^32). This limit could be reached for attributes such as hard drive sizes in bytes. The management point didn't process integer values above this limit, thus no value was stored in the database. Now in this release the limit is increased to 18,446,744,073,709,551,616 (2^64).

For more information, see Use of large integer values.

Hardware inventory default unit revision

In Configuration Manager version 1710, the default unit used in many reporting views changed from megabytes (MB) to gigabytes (GB). Due to improvements to hardware inventory for large integer values, and based on customer feedback, this default unit is now MB again.

Configuration Manager console

Product lifecycle dashboard

The product lifecycle dashboard shows the state of the Microsoft Lifecycle Policy for Microsoft products installed on devices managed with Configuration Manager. It also provides you with information about Microsoft products in your environment, supportability state, and support end dates. Use the dashboard to understand the availability of support for each product. This information helps you plan for when to update the Microsoft products you use before their current end of support is reached.

For more information, see Product lifecycle dashboard.

Copy asset details from monitoring views

The following areas of the **Monitoring** workspace now support copying text:

- In the **Deployments** node, select a deployment, and click **View Status**. In the **Asset Details** pane of the Deployment Status view, select one or more devices.
- Expand the **Distribution Status** node, and select **Content Status**. Select a piece of software, and click **View Status**. In the **Asset Details** pane of the Content Status view, select one or more distribution points.

Right-click the asset, and select **Copy**. This action copies the selected assets as a comma-delimited list that includes the full details. The keyboard shortcut **CTRL** + **C** also works in these views.

For more information, see Console improvements in version 1806.

Improvements to the Surface dashboard

This release includes the following improvements to the Surface dashboard:

- The Surface dashboard now displays a list of relevant devices when you select specific graph sections:
  - Clicking on the **Percent of Surface Devices** tile opens a list of Surface devices.
  - Clicking on a bar in the **Top Five Firmware Versions** tile opens a list of Surface devices with that specific firmware version.
- When viewing these device lists from the Surface dashboard, right-click a device to perform common actions.

For more information, see Surface dashboard.

View the currently signed on user for a device

Now by default the **Devices** node of the **Assets and Compliance** workspace displays a column for the **Currently logged on user**. It also displays for any collection-specific device list. This value is as current as the client status. When the user signs off, the client clears this value. If no user is signed on, the value is blank.

For more information, see Console improvements in version 1806.

Submit feedback from the Configuration Manager console

Send a smile! You can now directly tell the Configuration Manager team about your experiences. Sending feedback is easy from the Configuration Manager console. We want to hear all of your feedback: praise, problems, and suggestions. In the Configuration Manager console, click the smile button in the upper right corner above the ribbon. This feedback goes directly to the Microsoft product team for Configuration Manager. While using the

Windows 10 Feedback Hub is still supported, you're encouraged to use the in-console feedback mechanism.

For more information, see Console improvements in version 1806 and Product feedback.

Other updates

Aside from new features, this release also includes additional changes such as bug fixes. For more information, see Summary of changes in Configuration Manager current branch, version 1806.

For more information on changes to the Windows PowerShell cmdlets for Configuration Manager, see PowerShell 1806 Release Notes.

The following update rollup (4462978) is available in the console starting on 24 October 2018: Update rollup for Configuration Manager current branch, version 1806.

Hotfixes

The following additional hotfixes are available to address specific issues:

ID	TITLE	DATE	IN-CONSOLE
4346645	Update for System Center Configuration Manager version 1806, first wave	31 August 2018	Yes
4465865	Software updates do not download in Configuration Manager environment if WSUS is disconnected This update is also in the update rollup (4462978)	01 October 2018	Yes
4471892	PXE Responder doesn't work across subnets in Configuration Manager 1806	23 November 2018	No
4487960	Microsoft Intune connector certificate does not renew in Configuration Manager	18 January 2019	Yes

Next steps

When you're ready to install this version, see Installing updates for Configuration Manager and Checklist for installing update 1806.

> **TIP**
> To install a new site, use a baseline version of Configuration Manager.
>
> Learn more about:
>
> - Installing new sites
> - Baseline and update versions

For known, significant issues, see the Release notes.

After you update a site, also review the Post-update checklist.

What's new in version 1802 of System Center Configuration Manager

9/11/2019 • 14 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Update 1802 for Configuration Manager current branch is available as an in-console update. Apply this update on sites that run version 1702, 1706, or 1710. When installing a new site, it's also available as a baseline version.

Aside from new features, this release also includes additional changes such as bug fixes. For more information, see Summary of changes in System Center Configuration Manager current branch, version 1802.

The following additional updates to this release are also now available:

- Update rollup for System Center Configuration Manager current branch, version 1802

> **TIP**
> To install a new site, you must use a baseline version of Configuration Manager.
>
> Learn more about:
>
> - Installing new sites
> - Installing updates at sites
> - Baseline and update versions

The following sections provide details about the changes and new capabilities in version 1802 of Configuration Manager.

Site infrastructure

Reassign distribution point

Many customers have large Configuration Manager infrastructures, and are reducing primary or secondary sites to simplify their environment. They still need to retain distribution points at branch office locations to serve content to managed clients. These distribution points often contain multiple terabytes or more of content. This content is costly in terms of time and network bandwidth to distribute to these remote servers. This feature lets you reassign a distribution point to another primary site without redistributing the content. This action updates the site system assignment while persisting all of the content on the server. For more information, see Reassign a distribution point.

Configure Windows Delivery Optimization to use Configuration Manager boundary groups

You use Configuration Manager boundary groups to define and regulate content distribution across your corporate network and to remote offices. Windows Delivery Optimization is a cloud-based, peer-to-peer technology to share content between Windows 10 devices. Starting in this release, configure Delivery Optimization to use your boundary groups when sharing content among peers. A new client setting applies the boundary group identifier as the Delivery Optimization group identifier on the client. When the client communicates with the Delivery Optimization cloud service, it uses this identifier to locate peers with the desired content. For more information, see Fundamental concepts for content management.

Support for Windows 10 ARM64 devices

Starting in this release the Configuration Manager client is supported on Windows 10 ARM64 devices. Existing

client management features should work with these new devices. For example, hardware and software inventory, software updates, and application management. Operating system deployment is currently not supported.

Improved support for CNG certificates

Configuration Manager (current branch) version 1710 supports Cryptography: Next Generation (CNG) certificates. Version 1710 limits support to client certificates in several scenarios.

Starting in this release, use CNG certificates for the following HTTPS-enabled server roles:

- Management point
- Distribution point
- Software update point
- State migration point

Boundary group fallback for management points

Configure fallback relationships for management points between boundary groups. This behavior provides greater control for the management points that clients use. For more information, see Configure boundary groups.

Cloud distribution point site affinity

This feature benefits customers with a multi-site, geographically dispersed hierarchy using cloud distribution points. When an internet-based client searches for content, previously there was no order to the list of cloud distribution points received by the client. This behavior could result in internet-based clients receiving content from geographically distant cloud distribution points. Downloading content from such a distant server is typically slower than a closer server.

With cloud distribution point site affinity, an internet-based client receives an ordered list. This list prioritizes cloud distribution points from the client's assigned site. This behavior allows the administrator to preserve their design intent for content downloads from site resources.

Management insights

Management insights in System Center Configuration Manager provide information about the current state of your environment. The information is based on analysis of data from the site database. Insights help you to better understand your environment and take action based on the insight. For details see, Management Insights

In Configuration Manager 1802, the following insights are available:

- Applications:
  - Applications without deployments
- Cloud Services:
  - Assess co-management readiness
  - Enable your devices to be hybrid Azure Active Directory-joined
  - Modernize your identity and access infrastructure
  - Upgrade your clients to Windows 10, version 1709 or above
- Collections:
  - Empty Collections
- Simplified Management:
  - Outdated client versions
- Software Center:
  - Direct users to Software Center instead of Application Catalog
  - Use the new version of Software Center
- Windows 10:
  - Configure Windows telemetry and commercial ID key

- Connect Configuration Manager to Upgrade Readiness

Client management

Cloud management gateway support for Azure Resource Manager

When creating an instance of the cloud management gateway (CMG), the wizard now provides the option to create an **Azure Resource Manager deployment**. Azure Resource Manager is a modern platform for managing all solution resources as a single entity, called a resource group. When deploying CMG with Azure Resource Manager, the site uses Azure Active Directory (Azure AD) to authenticate and create the necessary cloud resources. This modernized deployment doesn't require the classic Azure management certificate. For more information, see CMG topology design.

> **IMPORTANT**
> This capability doesn't enable support for Azure Cloud Service Providers (CSP). The CMG deployment with Azure Resource Manager continues to use the classic cloud service, which the CSP doesn't support. For more information, see Available Azure services in Azure CSP.

Improvements to cloud management gateway

- Starting in this release, the **cloud management gateway** is no longer a pre-release feature.
- The feature documentation is revised and enhanced. For more information, see the following articles:
  - Plan for the cloud management gateway
  - Cloud management gateway size and scale numbers
  - Security and privacy for cloud management gateway
  - Frequently asked questions about the cloud management gateway
  - Certificates for cloud management gateway
  - Set up cloud management gateway

Configure hardware inventory to collect strings larger than 255 characters

You can configure the length of strings to be greater than 255 characters for hardware inventory properties. This change applies only to newly added classes and for hardware inventory properties that aren't keys. For details, see the Extend hardware inventory article.

Deprecation announcement for Linux and Unix client support

Microsoft intends to deprecate the Linux and UNIX client support in System Center Configuration Manager roughly one year from now, such that the clients will not be included in version 1902 in early calendar 2019. The Configuration Manager 1810 release, in late calendar 2018, will be the last release to include the Linux and UNIX clients, and they will be supported for the full lifecycle of Configuration Manager 1810. After Configuration Manager 1810, customers should consider Microsoft Azure Management for managing Linux servers. Azure solutions have extensive Linux support that in most cases exceed Configuration Manager functionality, including end-to-end patch management for Linux.

Surface device dashboard

The Surface device dashboard provides information about the Surface devices found in your environment. In the console, go to **Monitoring** > **Surface Devices**. You can view the items:

- Percent of Surfaces
- Percent of Surface models
- Top five firmware versions

For details, see the Surface dashboard article.

Change in the Configuration Manager client install

Starting in this release, Silverlight is no longer installed on client devices automatically. For more information, see Prerequisites for deploying clients to Windows computers

Co-management

Transition Endpoint Protection workload to Intune using co-management

The Endpoint Protection workload can be transitioned to Intune after enabling co-management. To transition the Endpoint Protection workload, go to the co-management properties page and move the slider bar from Configuration Manager to **Pilot** or **All**. For details about the workloads, see Co-management workloads. For more information about co-management, see Co-management for Windows 10 devices.

Co-management dashboard in System Center Configuration Manager

Beginning in this release, you can view a dashboard with information about co-management. The dashboard helps you review machines that are co-managed in your environment. The graphs can help identify devices that might need attention. For details, see the Co-management dashboard article.

Compliance settings

Microsoft Edge browser policies

For customers who use the Microsoft Edge web browser on Windows 10 clients, create a Configuration Manager compliance settings policy to configure several Microsoft Edge settings. For more information, see Create Microsoft Edge browser profile.

Application Management

Allow user interaction when installing an application

Allow an end user to interact with an application installation during the running of the task sequence. For example, run a setup process that prompts the end user for various options. Some application installers can't silence user prompts, or the installation process may require specific configuration values only known to the user. This feature allows you to handle these installation scenarios. For more information, see Specify user experience options for the deployment type.

Do not automatically upgrade superseded applications

Configure an application deployment to not automatically upgrade any superseded version. Now when creating the deployment, on the **Deployment Settings** page of the **Deploy Software Wizard**, for **Available** install purpose, you can enable or disable the option to **Automatically upgrade any superseded versions of this application**. For more information, see Specify deployment settings.

Approve application requests for users per device

Starting in this release, when a user requests an application that requires approval, the specific device name is now a part of the request. If the administrator approves the request, the user is only able to install the application on that device. The user must submit another request to install the application on another device. For more information, see Specify deployment settings.

> **NOTE**
> This is an optional feature. For more information, see Enable optional features from updates.

Run scripts improvements

Starting in this release, **Run Scripts** is no longer a pre-release feature. The script output now returns using JSON formatting. For more information, see Create and run PowerShell scripts from the Configuration Manager console.

Operating system deployment

Windows 10 in-place upgrade task sequence via cloud management gateway

The Windows 10 in-place upgrade task sequence now supports deployment to internet-based clients managed through the cloud management gateway. This ability allows remote users to more easily upgrade to Windows 10 without needing to connect to the corporate network. For more information, see Deploy a task sequence.

Improvements to Windows 10 in-place upgrade task sequence

The default task sequence template for Windows 10 in-place upgrade now includes additional groups with recommended actions to add before and after the upgrade process. These actions are common among many customers who are successfully upgrading devices to Windows 10. For more information, see create a task sequence to upgrade an OS.

Improvements to operating system deployment

This release includes the following improvements to operating system deployment:

- In Windows PE, when launching cmtrace.exe, you are no longer prompted to choose whether to make this program the default viewer for log files.
- Add boot images to the Download Package Content task sequence step.
- Improvements to the Run Task Sequence step:
  - Support for all operating system deployment scenarios from Software Center, PXE, and media.
  - Improvements to console actions such as copy, import, export, and warning during object deletion.
  - Support for the Create Prestaged Content File wizard.
  - Integration with deployment verification. For more information, see High-risk task sequence deployments.
  - The Run Task Sequence step can now be used across multiple levels of task sequences, not just a single parent-child relationship. Multi-level relationships increase the complexity, so use with caution. These relationships are still checked for circular references.

Deployment templates for task sequences

The deployment wizard for task sequences can now create a deployment template. The deployment template can be saved and applied to an existing or new task sequence to create a deployment.

Phased deployments for task sequences

Phased deployments is a pre-release feature. Phased deployments automate a coordinated, sequenced rollout of a task sequence across multiple collections. You can create phased deployments with the default of two phases, or manually configure multiple phases. Phased deployment of task sequences does not support PXE or media installation.

Software Center

Install multiple applications in Software Center

If an end user or desktop technician needs to install multiple applications on a device, Software Center now supports installing multiple selected applications. This behavior allows the user to be more efficient while not waiting for one installation to finish before starting the next. For more information, see Install multiple applications in the new Software Center user guide.

Use Software Center to browse and install user-available applications on Azure AD-joined devices

If you deploy applications as available to users, they can now browse and install them through Software Center on Azure Active Directory (Azure AD) devices. For more information, see Deploy user-available applications on Azure AD-joined devices.

Hide installed applications in Software Center

Installed applications can now be hidden in Software Center. Applications that are already installed will no longer show in the Applications tab when this option is enabled under client settings. This option is set as the default when you install or upgrade to Configuration Manager 1802. Installed applications are still available for review under the installation status tab. Hide installed applications in Software Center has additional details.

Hide unapproved applications in Software Center

When this client setting option is enabled, user available applications that require approval are hidden in Software Center. Hide unapproved applications in Software Center has additional details.

Software Center shows user additional compliance information

When using Device Health Attestation status as a compliance policy rule for conditional access to company resources, Software Center now shows the user the Device Health Attestation setting that is not compliant.

Software updates

Schedule automatic deployment rule evaluation to be offset from a base day.

Automatic deployment rules can be scheduled to evaluate offset from a base day. Meaning, if patch Tuesday actually falls on Wednesday for you, the evaluation schedule can be set for the second Tuesday of the month offset by one day. For details, see Automatically deploy software updates.

Reporting

Report for default browser counts

Now there is a new report to show the count of clients with a specific web browser as the Windows default. See the **Default Browser counts** report in the **Software - Companies and Products** reports group. For more information, see the List of reports.

Report on Windows Autopilot device information

Windows Autopilot is a solution for onboarding and configuring new Windows 10 devices in a modern way. For more information, see an Overview of Windows Autopilot. One method of registering existing devices with Windows Autopilot is to upload device information to the Microsoft Store for Business and Education. This information includes the device serial number, Windows product identifier, and a hardware identifier. Use Configuration Manager to collect and report this device information with the new report, **Windows Autopilot Device Information**, in the **Hardware - General** reports node. For more information, see How to prepare internet-based devices for co-management in preparing for co-management.

Report on Windows 10 Servicing details for a specific collection

The **Windows 10 Servicing details for a specific collection** report displays general information about Windows 10 servicing for a specific collection. This report shows Resource ID, NetBIOS name, OS name, OS release name, build, OS branch, and servicing state for Windows 10 devices. For more information, see the List of reports

Protect devices

Improvements to Configuration Manager Policies for Windows Defender Exploit Guard

Additional policy settings for the Attack Surface Reduction and Controlled folder access components have been added in Configuration Manager for Windows Defender Exploit Guard.

New host interaction settings for Windows Defender Application Guard

For Windows 10 version 1709 and later devices, there are two new host interaction settings for Windows Defender Application Guard:

- Websites can be given access to the host's virtual graphics processor.

- Files downloaded inside the container can be persisted on the host.

Configuration Manager console

Improvements to the Configuration Manager console

This release includes the following improvements to the Configuration Manager console.

- Device lists under Assets and Compliance, Devices, now display the primary user by default. This column only displays in the Devices node. The last logged on user can also be added as an optional column. Enable user and device affinity client settings for the site to associate a primary user with a device.
- If a collection is a member of another collection and it is renamed, then the new name is updated under membership rules.
- When using remote control on a client with multiple monitors at different DPI scaling, the mouse cursor now correctly maps between them.
- The Office 365 Client Management dashboard displays a list of relevant devices when graph sections are selected.

Next Steps

When you're ready to install this version, see Updates for Configuration Manager.

Removed and deprecated items for System Center Configuration Manager

7/19/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article describes how to use the information about features, products, and operating systems that are removed from support for System Center Configuration Manager, or will be removed in a future update (deprecated). This article provides early notice about future changes that might affect your use of Configuration Manager.

This information is subject to change with future releases, and might not include each deprecated feature, product, or operating system.

How to use this information

When a feature, product, or operating system is first listed as deprecated, support for using it with Configuration Manager is scheduled to be removed in a future version of Configuration Manager. This information is provided to help you plan for alternatives to using that feature, product, or operating system. When the first version of Configuration Manager releases in which that support is removed, this article is updated to indicate that specific version.

When support is removed for a feature or operating system, the feature or operating system remains supported when you use a previous version of Configuration Manager, as long as that version of Configuration Manager remains in support. However, when you use a version of Configuration Manager released after the date or version indicated, that version of Configuration Manager does not provide support.

For example, if a feature was scheduled to have its support removed with the first update released after September 2016, support for that feature would no longer be included in update 1610, which released in October of 2016.

- With Update 1610, the feature would no longer be supported.
- The article would be updated to indicate support was removed with version 1610. However, if you continue to use an earlier version that supports the feature, like version 1602 or 1606, you can continue to use that feature until the version you use drops out of support.

Removed and deprecated items for Configuration Manager

Items that are removed or deprecated are split between three categories.

Removed and deprecated Configuration Manager features

Removed and deprecated items for Configuration Manager site servers

Removed and deprecated items for Configuration Manager clients

More information

For more information, see:

- The Microsoft Support Lifecycle website.
- Support for current branch versions of Configuration Manager.

Removed and deprecated features for Configuration Manager

9/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article lists the features that are deprecated or removed from support for Configuration Manager. Deprecated features will be removed in a future update. These future changes might affect your use of Configuration Manager.

This information is subject to change with future releases. It might not include each deprecated Configuration Manager feature.

Deprecated features

The following features are deprecated. You can still use them now, but Microsoft plans to end support in the future.

FEATURE	DEPRECATION FIRST ANNOUNCED	SUPPORT REMOVED
Device health attestation assessment for conditional access compliance policies For more information, see Manage access to Office 365 services for PCs managed by Configuration Manager.	July 3, 2019	The first version released after November 1, 2019
The Configuration Manager Company Portal app	May 21, 2019	The first version released after November 1, 2019
The application catalog, including both site system roles: the application catalog website point and web service point. For more information, see Remove the application catalog.	May 21, 2019	The first version released after November 1, 2019
The implementation for sharing content from Azure has changed. Use a content-enabled cloud management gateway. You won't be able to create a traditional cloud distribution point in the future.	February 2019	TBD[Note 1]
Classic service deployment to Azure for cloud management gateway and cloud distribution point. For more information, see Plan for CMG.	November 2018	TBD[Note 1]
Windows Hello for Business settings in Configuration Manager For more information, see Windows Hello for Business settings.	December 2017	The first version released after November 1, 2019

Note 1: Support removed TBD

The specific timeframe is to be determined (TBD). Microsoft recommends that you change to the new process or

feature, but you can continue to use the deprecated process or feature for the near future.

Unsupported and removed features

The following features are no longer supported. In some cases, they're no longer in the product.

FEATURE	DEPRECATION FIRST ANNOUNCED	SUPPORT REMOVED
System Center Endpoint Protection for Mac and Linux For more information, see End of support blog post.	October 2018	December 31, 2018
On-premises conditional access For more information, see What is hybrid MDM.	January 30, 2019	September 1, 2019
Hybrid mobile device management (MDM) For more information, see What is hybrid MDM. Starting with the 1902 Intune service release, expected at the end of February 2019, new customers can't create a new hybrid connection.	August 14, 2018	September 1, 2019
The **Silverlight user experience** for the application catalog website point is no longer supported. Users should use the new Software Center. For more information, see Configure Software Center.	August 11, 2017	Version 1806
The previous version of Software Center. For more information about the new Software Center, see Plan for and configure application management.	December 13, 2016	Version 1802
Management of Virtual Hard Disks (VHDs) with Configuration Manager. This deprecation includes removal of options to create a new VHD or manage a VHD using a task sequence, and the removal of the Virtual Hard Disks node from the Configuration Manager console. Existing VHDs are not deleted, but are no longer accessible from within the Configuration Manager console.	January 6, 2017	Version 1710
Task sequences: - Convert Disk to Dynamic - Install Deployment Tools	November 18, 2016	Version 1710

FEATURE	DEPRECATION FIRST ANNOUNCED	SUPPORT REMOVED
System Center Configuration Manager Upgrade Assessment Tool. The Upgrade Assessment Tool depends on both System Center Configuration Manager and the Application Compatibility Toolkit (ACT) 6.x. The final version of ACT was shipped in the Windows 10 v1511 ADK. As there are no further updates to ACT, support for the Upgrade Assessment Tool is discontinued. The Upgrade Assessment Tool is replaced by the Upgrade Readiness feature. Deprecation notice was added to the download page for UAT on September 12, 2016.	September 12, 2016	July 11, 2017
Software update points with a network load balancing (NLB) cluster	February 27, 2016	Version 1702
Task sequences: - OSDPreserveDriveLetter During an operating system deployment, by default, Windows Setup now determines the best drive letter to use (typically C:). If you want to specify a different drive to use, you can change the location in the Apply Operating System task sequence step. Go to the **Select the location where you want to apply this operating system** setting. Select **Specific logical drive letter** and choose the drive that you want to use.	June 20, 2016	Version 1606
Network Access Protection (NAP) - as found in System Center 2012 Configuration Manager	July 10, 2015	Version 1511
Out of Band Management - as found in System Center 2012 Configuration Manager	October 16, 2015	Version 1511

Features removed in version 1511

The following sections include additional details for features removed with version 1511:

Out of Band Management

With Configuration Manager, native support for AMT-based computers from within the Configuration Manager console has been removed.

- AMT-based computers remain fully managed when you use the Intel SCS Add-on for Microsoft System Center Configuration Manager. The add-on provides you access to the latest capabilities to manage AMT, while removing limitations introduced until Configuration Manager could incorporate those changes.
- Out of Band Management in System Center 2012 Configuration Manager is not affected by this change.

Network Access Protection

System Center Configuration Manager has removed support for Network Access Protection. The feature has been deprecated in Windows Server 2012 R2, and is removed from Windows 10.

For network access protection alternatives, see the *Deprecated functionality* section of Network Policy and Access Services Overview.

See also

- Removed and deprecated
- Microsoft Support Lifecycle
- Support for current branch versions of Configuration Manager

Removed and deprecated for Configuration Manager site servers

6/20/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article describes products and operating systems that are removed from support for Configuration Manager site servers, or will be removed in a future update (deprecated). It provides early notice about future changes that might affect your use of Configuration Manager.

This information may change in the future. It might not include each deprecated feature, product, or operating system.

Server OS

OPERATING SYSTEMS	DEPRECATION FIRST ANNOUNCED	SUPPORT REMOVED
Windows Server 2008 R2 with SP1	July 10, 2015	Version 1702 Note 1
Windows Server 2008 with SP2	July 10, 2015	Version 1511 Note 2

Note 1: Windows Server 2008 R2 with SP1

Windows Server 2008 R2 with Service Pack 1 isn't supported for site servers or most site system roles. This OS is still supported for the distribution point role. This support includes pull-distribution points, PXE, and multicast.

> **IMPORTANT**
> The extended support end date for Windows Server 2008 R2 with SP1 is January 14, 2020. After this date, Configuration Manager won't support this OS as any site system role.

You can upgrade the site server OS from Windows Server 2008 R2 to Windows Server 2012 R2. For more information, see In-place upgrade the operating system of site servers that run Windows Server 2008 R2.

Note 2: Windows Server 2008 with SP2

Windows Server 2008 with Service Pack 2 isn't supported for site servers or most site system roles. This OS is still supported for the distribution point role. This support includes pull-distribution points, PXE, and multicast.

> **IMPORTANT**
> The extended support end date for Windows Server 2008 with SP2 is January 14, 2020. After this date, Configuration Manager won't support this OS as any site system role.

SQL Server

SQL SERVER VERSIONS	DEPRECATION FIRST ANNOUNCED	SUPPORT REMOVED
SQL Server 2008 R2	July 10, 2015	Version 1702

SQL SERVER VERSIONS	DEPRECATION FIRST ANNOUNCED	SUPPORT REMOVED
SQL Server 2008	July 10, 2015	Version 1511

If you need to upgrade your version of SQL Server, we recommend the following methods, from easy to more complex:

1. Upgrade SQL Server in-place (recommended).
2. Install a new version of SQL Server on a new computer. Then to point your site server at the new SQL Server, use the database move option of Configuration Manager setup.
3. Use backup and recovery.

More information

For more information, see the following articles:

- Removed and deprecated
- Microsoft Support Lifecycle
- Support for current branch versions of Configuration Manager

Removed and deprecated items for Configuration Manager clients

7/26/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article describes products and operating systems that are removed from support for Configuration Manager clients, or will be removed in a future update (deprecated). It provides early notice about future changes that might affect your use of Configuration Manager.

This information may change in the future. It might not include each deprecated feature, product, or operating system.

Deprecated client operating systems

Unless noted otherwise, each supported OS is supported as a Configuration Manager client until the *Extended Support End Date* of that OS version. For more information about extended support end dates, see the Microsoft Support Lifecycle. If Configuration Manager support for an OS ends before the extended support end date, this article lists a deprecation date and support removal date for that OS.

OPERATING SYSTEMS	DEPRECATION FIRST ANNOUNCED	SUPPORT REMOVED
Windows CE 7.0	July 19, 2019	The first version released after June 30, 2020
Windows 10 Mobile	July 19, 2019	The first version released after June 30, 2020
Windows 10 Mobile Enterprise	July 19, 2019	The first version released after June 30, 2020
Linux and UNIX	March 22, 2018	Version 1902
Windows 8: Professional, Enterprise	January 12, 2016	Version 1802
Windows Embedded 8 Pro	January 12, 2016	Version 1802
Windows Embedded 8 Industry	January 12, 2016	Version 1802
Windows XP Embedded Includes all XP-based embedded operating systems	July 10, 2015	Version 1702
Windows Vista	July 10, 2015	Version 1511
Windows Server 2003 R2	July 10, 2015	Version 1511
Windows Server 2003	July 10, 2015	Version 1511

OPERATING SYSTEMS	DEPRECATION FIRST ANNOUNCED	SUPPORT REMOVED
Windows XP	July 10, 2015	Version 1511
Mac OS X 10.6 - 10.8	July 10, 2015	Version 1511
Windows Mobile 6.0 - 6.5	July 10, 2015	Version 1511
Nokia Symbian Belle	July 10, 2015	Version 1511
Windows CE 5.0 - 6.0	July 10, 2015	Version 1511

See also

For more information, see the following articles:

- Removed and deprecated
- Microsoft Support Lifecycle
- Support for current branch versions of Configuration Manager

Supported configurations for System Center Configuration Manager

9/5/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

As an on-premises solution, System Center Configuration Manager makes use of your servers, clients, network configurations, and additional products like Microsoft Intune, SQL Server, and Azure.

The information in this and the following topics is essential for helping you identify key configurations, requirements, and limitations, so that you can plan, deploy, and maintain a functional Configuration Manager deployment. This information is specific to the infrastructure for Configuration Manager sites, hierarchies, and managed devices.

When a Configuration Manager feature or capability requires more specific configurations, that information is included with the feature-specific documentation, and is supplemental to the more general configuration details.

The products and technologies that are described in the following topics are supported by Configuration Manager. However, their inclusion in this content does not imply an extension of support for any product beyond that product's individual support lifecycle. Products that are beyond their support lifecycle are not supported for use with Configuration Manager. For more information about Microsoft Support Lifecycles, visit the Microsoft Support Lifecycle website.

> **NOTE**
> For information about Microsoft support lifecycle policy, go to the Microsoft Support Lifecycle Support Policy FAQ website at Microsoft Support Lifecycle Policy FAQ.

Additionally, products and product versions that are not listed in the following topics are not supported with System Center Configuration Manager unless they have been announced on the Enterprise Mobility and Security Blog. At times, the content on this blog precedes an update to this body of documentation.

- Size and scale numbers
  Learn about how many sites, site system roles per site, and clients or devices are supported in different hierarchy designs for Configuration Manager.
- Site and site system prerequisites
  Learn about configurations that are required on a Windows Server to support different site types and site system roles.
- Supported operating systems for site system servers
  Learn about which operating systems you can use as a site server or site system server.
- Supported operating systems for clients and devices
  Learn about which operating systems you can manage with Configuration Manager, including Windows, Windows Embedded, Linux and UNIX, Mac, and mobile devices.
- Supported operating systems for the console
  Learn about which operating systems can host the Configuration Manager console to provide a point of access for managing your deployment.
- Support for SQL Server versions

Learn about which versions of SQL Server can host the site database and reporting database, as well as about required configurations and optional configurations that you can use.

- High-availability options
  Learn about the options you can implement when designing your environment to help maintain a high level of available service for your Configuration Manager deployment.
- Recommended hardware
  Learn about guidelines that can help you identify the right hardware and configurations to host your Configuration Manager sites and key services.
- Support for Active Directory domains
  Learn about the supported Active Directory domain configurations that Configuration Manager requires and supports.
- Support for Windows features and networks
  Learn about supported Windows technologies (such as BranchCache and data deduplication) and limitations for their use with Configuration Manager.
- Support for virtualization environments
  Learn more about how to use supported virtual machine technologies.

Size and scale numbers for Configuration Manager

8/19/2019 • 10 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Each Configuration Manager deployment has a maximum number of sites, site system roles, and devices that it can support. These numbers vary depending on your hierarchy structure, what types and numbers of sites you use, and the site system roles that you deploy. The information in this article can help you determine the number of site system roles and sites that you need to support the devices you expect to manage.

For more information, see the following articles:

- Recommended hardware
- Supported operating systems for site system servers
- Supported operating systems for clients and devices
- Site and site system prerequisites

These support numbers are based on using the recommended hardware for Configuration Manager. They're also based on the default settings for all available Configuration Manager features. When you don't use the recommended hardware or use more aggressive custom settings, the performance of site systems can degrade. The site systems might not meet the stated levels of support. (An example of more aggressive client settings is running hardware or software inventory more frequently than the defaults of once every seven days.)

Site types

Central administration site

- A central administration site supports up to 25 child primary sites.

Primary site

- Each primary site supports up to 250 secondary sites.
- The number of secondary sites per primary site is based on continuously connected and reliable wide area network (WAN) connections. For locations that have fewer than 500 clients, consider a distribution point instead of a secondary site.

  For information about the number of clients and devices that a primary site can support, see Client numbers for sites and hierarchies.

Secondary site

- Secondary sites don't support child sites.

Site system roles

Application catalog web service point

> **IMPORTANT**
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features

- You can install multiple instances of the Application Catalog web service point at primary sites.

Application catalog website point

> **IMPORTANT**
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features

- You can install multiple instances of the Application Catalog website point at primary sites.

Cloud management gateway

- You can install multiple instances of the cloud management gateway (CMG) at primary sites, or the central administration site.

  > **TIP**
  > In a hierarchy, create the CMG at the central administration site.

  - One CMG supports one to 16 virtual machine (VM) instances in the Azure cloud service.
  - Each CMG VM instance supports 6,000 simultaneous client connections. When the CMG is under high load due to more than the supported number of clients, it still handles requests but there may be delay.

For more information, see CMG Performance and scale

Cloud management gateway connection point

- You can install multiple instances of the CMG connection point at primary sites.
- One CMG connection point can support a CMG with up to four VM instances. If the CMG has more than four VM instances, add a second CMG connection point for load balancing. A CMG with 16 VM instances should be linked with four CMG connection points.

For more information, see CMG Performance and scale

Distribution point

- Distribution points per site:

- Each primary and secondary site supports up to 250 distribution points.
- Each primary and secondary site supports up to 2000 additional distribution points that are configured as pull-distribution points. **For example**, a single primary site supports 2250 distribution points when 2000 of those distribution points are configured as pull-distribution points.
- Each distribution point supports connections from up to 4,000 clients.
- A pull-distribution point acts like a client when it accesses content from a source distribution point.

- Each primary site supports a combined total of up to 5,000 distribution points. This total includes all the distribution points at the primary site and all the distribution points that belong to the primary site's child secondary sites.
- Each distribution point supports a combined total of up to 10,000 packages and applications.

> **WARNING**
> The actual number of clients that one distribution point can support depends on the speed of the network and the hardware configuration of the server.
>
> The number of pull-distribution points that one source distribution point can support similarly depends on the speed of the network and the hardware configuration of the source distribution point. But this number is also affected by the amount of content that you've deployed. This effect is because, unlike clients that typically access content at different times during a deployment, all pull-distribution points request content at the same time. Pull-distribution points can request all available content, not just the content that is applicable to them. When you place a high processing load on a source distribution point, there can be unexpected delays in distributing the content to the target distribution points.

Fallback status point

- Each fallback status point can support up to 100,000 clients.

Management point

- Each primary site supports up to 15 management points.

> **TIP**
> Don't install management points on servers that are across a slow link from the primary site server or the site database server.

- Each secondary site supports a single management point that must be installed on the secondary site server.

For information about the number of clients and devices that a management point can support, see the Management points section.

Software update point

Use the following recommendations as a baseline. This baseline helps you determine the information for the software updates capacity planning that is appropriate to your organization. The actual capacity requirements might vary from the recommendations listed in this article depending on the following criteria:

- Your specific networking environment
- The hardware that you use to host the software update point site system
- The number of managed clients
- The other site system roles installed on the server

Capacity planning for the software update point

The number of supported clients depends on the version of Windows Server Update Services (WSUS) that runs on the software update point. It also depends on whether the software update point site system role coexists with another site system role:

- The software update point can support up to 25,000 clients when WSUS runs on the software update point server, and the software update point coexists with another site system role.
- The software update point can support up to 150,000 clients when a remote server meets WSUS requirements, WSUS is used with Configuration Manager, and you configure the following settings:

  IIS Application Pools:

  - Increase the WsusPool Queue Length to 2000
  - Increase the WsusPool Private Memory limit x4 times, or set to 0 (unlimited). For example, if the default limit is 1,843,200 KB, increase it to 7,372,800. For more information, see this Configuration Manager support team blog post.

  For more information about hardware requirements for the software update point, see Recommended hardware for site systems.

Capacity planning for software updates objects

Use the following capacity information to plan for software updates objects:

- **Limit of 1000 software updates in a deployment** -Limit the number of software updates to 1000 for each software update deployment. When you create an automatic deployment rule (ADR), specify criteria that limits the number of software updates. The ADR fails when the specified criteria returns more than 1000 software updates. Check the status of the ADR from the **Automatic Deployment Rules** node in the Configuration Manager console. When you manually deploy software updates, don't select more than 1000 updates to deploy.

  Also limit the number of software updates to 1000 in a configuration baseline. For more information, see Create configuration baselines.

- **Limit of 580 security scopes for automatic deployment rules** - Limit the number of security scopes on automatic deployment rules (ADRs) to less than 580. When you create an ADR, the security scopes that have access to it are automatically added. If there are more than 580 security scopes set, the ADR will fail to run and an error is logged in ruleengine.log.

Client numbers for sites and hierarchies

Use the following information to determine how many clients and which types of clients you can support at a site or in a hierarchy.

Hierarchy with a central administration site

A central administration site supports a total number of devices that includes up to the number of devices listed for the following three groups:

- 700,000 Windows desktops. Also see support for embedded devices.
- 25,000 devices that run Mac and Windows CE 7.0
- One of the following, depending on how your deployment supports mobile device management (MDM):
  - 100,000 devices that you manage by using on-premises MDM
  - 300,000 cloud-based devices

For example, in a hierarchy you can support 700,000 desktops, up to 25,000 Mac and Windows CE 7.0 devices, and up to 300,000 cloud-based devices when you integrate Microsoft Intune. This hierarchy supports a total of

1,025,000 devices. If you support devices that are managed by on-premises MDM, the total for this hierarchy is 825,000 devices.

> **IMPORTANT**
> In a hierarchy where the central administration site uses a Standard edition of SQL Server, the hierarchy supports a maximum of 50,000 desktops and devices. To support more than 50,000 desktops and devices, you must use an Enterprise edition of SQL Server. This requirement applies only to a central administration site. It doesn't apply to a stand-alone primary site or a child primary site. The edition of SQL Server you use for a primary site doesn't limit its capacity to support the stated number of clients.

The edition of SQL Server that is in use at a stand-alone primary site doesn't limit that site's capacity to support up to the stated number of clients.

Child primary site

Each child primary site in a hierarchy with a central administration site supports the following number of clients:

- 150,000 total clients and devices that aren't limited to a specific group or type, as long as support doesn't exceed the number that is supported for the hierarchy. Also see, support for embedded devices.

For example, a primary site supports 25,000 Mac and Windows CE 7.0 devices. That number is the limit for a hierarchy. This primary site can then support an additional 125,000 desktop computers. The total number of supported devices for the child primary site is the supported maximum limit of 150,000.

Stand-alone primary site

A stand-alone primary site supports the following number of devices:

- 175,000 total clients and devices, not to exceed:
  - 150,000 desktops (computers that run Windows, Linux, and UNIX). Also see, support for embedded devices.
  - 25,000 devices that run Mac and Windows CE 7.0
  - One of the following, depending on how your deployment supports mobile device management:
    - 50,000 devices that you manage by using on-premises MDM
    - 150,000 cloud-based devices

For example, a stand-alone primary site that supports 150,000 desktops and 10,000 Mac or Windows CE 7.0 can support only an additional 15,000 devices. Those devices can be either cloud-based or managed by using on-premises MDM.

Primary sites and Windows Embedded devices

Primary sites support Windows Embedded devices that have File-Based Write Filters (FBWF) enabled. When embedded devices don't have write filters enabled, a primary site can support a number of embedded devices up to the allowed number of devices for that site. When embedded devices have FBWF or Unified Write Filters (UWF) enabled, a primary site can support a maximum of 10,000 Windows embedded devices. These devices must be configured with the exceptions listed in the important note found in the Planning for client deployment to Windows Embedded devices. A primary site supports only 3,000 Windows Embedded devices that have EWF enabled and that are not configured for the exceptions.

Secondary sites

Secondary sites support the following number of devices:

- 15,000 desktops (computers that run Windows, Linux, and UNIX)

Management points

Each management point can support the following number of devices:

- 25,000 total clients and devices, not to exceed:
  - 25,000 desktops (computers that run Windows, Linux, and UNIX)
  - One of the following (not both):
    - 10,000 devices that are managed by using on-premises MDM
    - 10,000 devices that run Mac and Windows CE 7.0 clients

Site and site system prerequisites for Configuration Manager

8/1/2019 • 20 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Windows-based computers require specific configurations to support their use as Configuration Manager site system servers.

This article primarily focuses on Windows Server 2012 and later. Windows Server 2008 R2 and Windows Server 2008 are supported for the distribution point site system role. For more information, see Supported operating systems for site system servers.

For some products, like Windows Server Update Services (WSUS) for the software update point, you need to refer to the product documentation to identify additional prerequisites and limitations for use. Only configurations that directly apply for use with Configuration Manager are included here.

For more information on .NET Framework, see Lifecycle FAQ - .NET Framework.

General requirements and limitations

The following requirements apply to all site system servers:

- Each site system server must use a 64-bit OS. The only exception is the distribution point site system role, which you can install on some 32-bit operating systems.
- Site systems aren't supported on Server Core installations of any operating system. An exception is that Server Core installations are supported for the distribution point site system role. For more information, see Supported operating systems for Configuration Manager site system servers.
- After a site system server is installed, it's not supported to change:
  - The domain name of the domain where the site system computer is located (also called a **domain rename**).
  - The domain membership of the computer.
  - The name of the computer.

  If you must change any of these items, first remove the site system role from the computer. Then reinstall the role after the change is complete. For changes affecting the site server, first uninstall the site. Then reinstall the site after the change is complete.
- Site system roles aren't supported on an instance of a Windows Server cluster. The only exception is the site database server. For more information, see Use a SQL Server cluster for the Configuration Manager site database.

  Starting in version 1810, the Configuration Manager setup process no longer blocks installation of the site server role on a computer with the Windows role for Failover Clustering. SQL Always On requires this role, so previously you couldn't colocate the site database on the site server. With this change, you can create a highly available site with fewer servers by using SQL Always On and a site server in passive mode. For more information, see High availability options.
- It's not supported to change the startup type or "Log on as" settings for any Configuration Manager

service. If you do, you might prevent key services from running correctly.

Prerequisites for Windows Server 2012 and later operating systems

See the main sections of this article for the specific prerequisites for site system servers and roles on Windows Server 2012 and later:

- Central administration site and primary site servers
- Secondary site server
- Database server
- SMS Provider server
- Application Catalog website point
- Application Catalog web service point
- Asset Intelligence synchronization point
- Certificate registration point
- Distribution point
- Endpoint Protection point
- Enrollment point
- Enrollment proxy point
- Fallback status point
- Management point
- Reporting services point
- Service connection point
- Software update point
- State migration point

Central administration site and primary site servers

Windows Server roles and features

- .NET Framework 3.5
- Remote Differential Compression

.NET Framework

Enable the Windows feature for .NET Framework 3.5.

Also install a supported version of the .NET Framework version 4.5 or later. Starting in version 1906, Configuration Manager supports .NET Framework 4.8.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

Windows ADK

- Before you install or upgrade a central administration site or primary site, install the version of the Windows Assessment and Deployment Kit (ADK) that's required by the version of Configuration Manager you're installing or upgrading to. For more information, see Windows 10 ADK.
- For more information about this requirement, see Infrastructure requirements for OS deployment.

Visual C++ Redistributable

- Configuration Manager installs the Microsoft Visual C++ 2013 Redistributable Package on each computer that installs a site server.

- Central administration sites and primary sites require both the x86 and x64 versions of the applicable redistributable file.

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Secondary site server

Windows Server roles and features

- .NET Framework 3.5
- Remote Differential Compression

.NET Framework

Enable the Windows feature for .NET Framework 3.5.

Also install a supported version of the .NET Framework version 4.5 or later. Starting in version 1906, Configuration Manager supports .NET Framework 4.8.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

Visual C++ Redistributable

- Configuration Manager installs the Microsoft Visual C++ 2013 Redistributable Package on each computer that installs a site server.
- Secondary sites require only the x64 version.

Default site system roles

- By default, a secondary site installs a **management point** and a **distribution point**.
- Ensure that the secondary site server meets the prerequisites for these site system roles.

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Database server

Remote Registry service

- During installation of the Configuration Manager site, enable the **Remote Registry** service on the computer that hosts the site database.

SQL Server

- Before you install a central administration site or primary site, install a supported version of SQL Server to host the site database. For more information, see Supported SQL Server versions.
- Before you install a secondary site, you can install a supported version of SQL Server.
- If you choose to have Configuration Manager install SQL Server Express as part of the secondary site

installation, ensure that the computer meets the requirements to run SQL Server Express.

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

SMS Provider server

Windows ADK

- The computer where you install an instance of the SMS Provider must have the required version of the Windows ADK that the version of Configuration Manager you're installing or upgrading to requires. For more information, see Windows 10 ADK.
- For more information about this requirement, see Infrastructure requirements for operating system deployment.

Windows Server roles and features

- If you're using the administration service, the server that hosts the SMS Provider role requires .NET 4.5.2 or later
  - Starting in version 1902, this prerequisite is version .NET 4.5 or later.
- Web Server (IIS): Every provider attempts to install the administration service. This service has a dependency on IIS to bind a certificate to HTTPS port 443. Configuration Manager uses IIS APIs to check this certificate configuration. If you configure the site for Enhanced HTTP, Configuration Manager uses IIS APIs to bind the SCCM-generated certificate.

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Application catalog website point

> **IMPORTANT**
>
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features

Windows Server roles and features

- .NET Framework 3.5
- ASP.NET 4.5

.NET Framework

Enable the Windows feature for .NET Framework 3.5.

Also install a supported version of the .NET Framework version 4.5 or later.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

IIS configuration

- Common HTTP Features:
  - Default Document
  - Static Content
- Application Development:
  - ASP.NET 3.5 (and automatically selected options)
  - ASP.NET 4.5 (and automatically selected options)
  - .NET Extensibility 3.5
  - .NET Extensibility 4.5
- Security:
  - Windows Authentication
- IIS 6 Management Compatibility:
  - IIS 6 Metabase Compatibility

Application catalog web service point

> **IMPORTANT**
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features

Windows Server roles and features

- .NET Framework 3.5
- ASP.NET 4.5:
  - HTTP Activation (and automatically selected options)

.NET Framework

Enable the Windows feature for .NET Framework 3.5.

Also install a supported version of the .NET Framework version 4.5 or later.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies

- Lifecycle FAQ - .NET Framework

IIS configuration

- Common HTTP Features:
  - Default Document
- IIS 6 Management Compatibility:
  - IIS 6 Metabase Compatibility
- Application Development:
  - ASP.NET 3.5 (and automatically selected options)
  - .NET Extensibility 3.5
  - ASP.NET 4.5 (and automatically selected options)
  - .NET Extensibility 4.5

Computer memory

- The computer that hosts this site system role must have a minimum of 5% of the computer's available memory free to enable the site system role to process requests.
- When this site system role is colocated with another site system role that has this same requirement, this memory requirement for the computer doesn't increase, but remains at a minimum of 5%.

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Asset Intelligence synchronization point

.NET Framework

Install a supported version of the .NET Framework version 4.5 or later. Starting in version 1906, Configuration Manager supports .NET Framework 4.8.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Certificate registration point

Windows Server roles and features

- .NET Framework
  - HTTP Activation

.NET Framework

Install a supported version of the .NET Framework version 4.5 or later. Starting in version 1906, Configuration Manager supports .NET Framework 4.8.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

IIS configuration

- Application Development:
  - ASP.NET 3.5 (and automatically selected options)
  - ASP.NET 4.5 (and automatically selected options)
- IIS 6 Management Compatibility:
  - IIS 6 Metabase Compatibility
  - IIS 6 WMI Compatibility

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Distribution point

Windows Server roles and features

- Remote Differential Compression

IIS configuration

- Application Development:
  - ISAPI Extensions
- Security:
  - Windows Authentication
- IIS 6 Management Compatibility:
  - IIS 6 Metabase Compatibility
  - IIS 6 WMI Compatibility

PowerShell

- On Windows Server 2012 or later, PowerShell 3.0 or 4.0 is required before you install the distribution point.

Visual C++ Redistributable

- Configuration Manager installs the Microsoft Visual C++ 2013 Redistributable Package on each computer that hosts a distribution point.
- The version that's installed depends on the computer's platform (x86 or x64).

Microsoft Azure

- You can use a cloud service in Microsoft Azure to host a distribution point.

To support PXE or multicast

- Install and configure the Windows Deployment Services (WDS) Windows Server role.

> **NOTE**
> WDS installs and configures automatically when you configure a distribution point to support PXE or multicast on a server that runs Windows Server 2012 or later.

- Starting in version 1806, enable a PXE responder on a distribution point without Windows Deployment Service.
- For a multicast-enabled distribution point, make sure the SQL Server Native Client is installed and up to date. For more information, see Prerequisite checks - SQL Server Native Client.

For more information, see Install and configure distribution points.

> **NOTE**
> When the distribution point transfers content, it transfers using the **Background Intelligent Transfer Service** (BITS) built into Windows. The distribution point role doesn't require the optional BITS IIS Server Extension feature to be installed, because the client doesn't upload information to it.

Endpoint Protection point

Windows Server roles and features

- .NET Framework 3.5
- Windows Defender features (Windows Server 2016 or later)

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Enrollment point

Windows Server roles and features

- .NET Framework 3.5
  - HTTP Activation (and automatically selected options)
  - ASP.NET 4.5
  - Windows Communication Foundation (WCF) Services

.NET Framework

Enable the Windows feature for .NET Framework 3.5.

Also install a supported version of the .NET Framework version 4.5 or later. Starting in version 1906, Configuration Manager supports .NET Framework 4.8.

> **NOTE**
> When this site system role installs, Configuration Manager automatically installs the .NET Framework 4.5.2. This installation can place the server into a reboot pending state. If a reboot is pending for the .NET Framework, .NET applications might fail until after the server reboots and the installation finishes.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

IIS configuration

- Common HTTP Features:
  - Default Document
- Application Development:
  - ASP.NET 3.5 (and automatically selected options)
  - .NET Extensibility 3.5
  - ASP.NET 4.5 (and automatically selected options)
  - .NET Extensibility 4.5
- IIS 6 Management Compatibility:
  - IIS 6 Metabase Compatibility

Computer memory

- The computer that hosts this site system role must have a minimum of 5% of the computer's available memory free to enable the site system role to process requests.
- When this site system role is colocated with another site system role that has this same requirement, this memory requirement for the computer doesn't increase, but remains at a minimum of 5%.

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Enrollment proxy point

Windows Server roles and features

- .NET Framework 3.5

.NET Framework

Enable the Windows feature for .NET Framework 3.5.

Also install a supported version of the .NET Framework version 4.5 or later. Starting in version 1906, Configuration Manager supports .NET Framework 4.8.

> **NOTE**
> When this site system role installs, Configuration Manager automatically installs the .NET Framework 4.5.2. This installation can place the server into a reboot pending state. If a reboot is pending for the .NET Framework, .NET applications might fail until after the server reboots and the installation finishes.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

IIS configuration

- Common HTTP Features:
  - Default Document
  - Static Content
- Application Development:
  - ASP.NET 3.5 (and automatically selected options)
  - ASP.NET 4.5 (and automatically selected options)
  - .NET Extensibility 3.5
  - .NET Extensibility 4.5
- Security:
  - Windows Authentication
- IIS 6 Management Compatibility:
  - IIS 6 Metabase Compatibility

Computer memory

- The computer that hosts this site system role must have a minimum of 5% of the computer's available memory free to enable the site system role to process requests.
- When this site system role is colocated with another site system role that has this same requirement, this memory requirement for the computer doesn't increase, but remains at a minimum of 5%.

Fallback status point

Windows Server roles and features

- BITS Server Extensions (and automatically selected options) or Background Intelligent Transfer Services (BITS) (and automatically selected options)

IIS configuration

The default IIS configuration is required with the following additions:

- IIS 6 Management Compatibility:
  - IIS 6 Metabase Compatibility

Management point

Windows Server roles and features

- BITS Server Extensions (and automatically selected options) or Background Intelligent Transfer Services (BITS) (and automatically selected options)

.NET Framework

Install a supported version of the .NET Framework version 4.5 or later. Starting in version 1906, Configuration Manager supports .NET Framework 4.8.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

IIS configuration

- Application Development:
  - ISAPI Extensions
- Security:
  - Windows Authentication
- IIS 6 Management Compatibility:
  - IIS 6 Metabase Compatibility
  - IIS 6 WMI Compatibility

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Reporting services point

.NET Framework

Install a supported version of the .NET Framework version 4.5 or later. Starting in version 1906, Configuration Manager supports .NET Framework 4.8.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

SQL Server Reporting Services

- Install and configure at least one instance of SQL Server to support SQL Server Reporting Services before installing the reporting point.
- The instance that you use for SQL Server Reporting Services can be the same instance you use for the site database.
- Additionally, the instance that you use can be shared with other System Center products, as long as the other System Center products don't have restrictions for sharing the instance of SQL Server.

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Service connection point

.NET Framework

Enable the Windows feature for .NET Framework 3.5.

Also install a supported version of the .NET Framework version 4.5 or later. Starting in version 1906, Configuration Manager supports .NET Framework 4.8.

> **NOTE**
> When this site system role installs, Configuration Manager automatically installs the .NET Framework 4.5.2. This installation can place the server into a reboot pending state. If a reboot is pending for the .NET Framework, .NET applications might fail until after the server reboots and the installation finishes.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

Visual C++ Redistributable

- Configuration Manager installs the Microsoft Visual C++ 2013 Redistributable Package on each computer that hosts a distribution point.
- The site system role requires the x64 version.

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Software update point

Windows Server roles and features

- .NET Framework 3.5

The default IIS configuration is required.

.NET Framework

Enable the Windows feature for .NET Framework 3.5.

Also install a supported version of the .NET Framework version 4.5 or later. Starting in version 1906, Configuration Manager supports .NET Framework 4.8.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

Windows Server Update Services

- Install the Windows server role Windows Server Update Services on a computer before installing a software update point.
- For more information, see Plan for software updates.

> **NOTE**
> When you use a Software Update Point on a server other than the site server, you must install the WSUS Administration Console on the site server.

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native

Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

State migration point

Windows Server roles and features

- .NET Framework 3.5
  - HTTP Activation (and automatically selected options)
  - ASP.NET 4.5

.NET Framework

Enable the Windows feature for .NET Framework 3.5.

Also install a supported version of the .NET Framework version 4.5 or later. Starting in version 1906, Configuration Manager supports .NET Framework 4.8.

> **NOTE**
> When this site system role installs, Configuration Manager automatically installs the .NET Framework 4.5.2. This installation can place the server into a reboot pending state. If a reboot is pending for the .NET Framework, .NET applications might fail until after the server reboots and the installation finishes.

For more information about .NET Framework versions, see the following articles:

- .NET Framework versions and dependencies
- Lifecycle FAQ - .NET Framework

IIS configuration

- Common HTTP Features:
  - Default Document
- Application Development:
  - ASP.NET 3.5 (and automatically selected options)
  - .NET Extensibility 3.5
  - ASP.NET 4.5 (and automatically selected options)
  - .NET Extensibility 4.5
- IIS 6 Management Compatibility:
  - IIS 6 Metabase Compatibility

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Make sure this component is up to date. For more information, see Prerequisite checks - SQL Server Native Client.

Prerequisites for Windows Server 2008 R2 and Windows Server 2008

Windows Server 2008 and Windows Server 2008 R2 are now in extended support and are no longer in mainstream support, as detailed by the Microsoft Support Lifecycle. For more information about future support

for these operating systems as site system servers with Configuration Manager, see Removed and deprecated server operating systems.

These OS versions aren't supported for site servers or most site system roles. They're still supported for the distribution point site system role, including pull-distribution points and for PXE and multicast.

Distribution point

IIS configuration

You can use the default IIS configuration or a custom configuration. To use a custom IIS configuration, you must enable the following options for IIS:

- Application Development:
  - ISAPI Extensions
- Security:
  - Windows Authentication
- IIS 6 Management Compatibility:
  - IIS 6 Metabase Compatibility
  - IIS 6 WMI Compatibility

When you use a custom IIS configuration, you can remove options that aren't required, such as the following items:

- Common HTTP Features:
  - HTTP Redirection
- IIS Management Scripts and Tools

Windows feature

- Remote Differential Compression

Visual C++ Redistributable

- Configuration Manager installs the Microsoft Visual C++ 2013 Redistributable Package on each computer that hosts a distribution point.
- The version that is installed depends on the computer's platform (x86 or x64).

To support PXE or multicast

- Install and configure the Windows Deployment Services (WDS) Windows Server role.

  > **NOTE**
  > WDS installs and configures automatically when you configure a distribution point to support PXE or multicast on a server that runs Windows Server 2012 or later.

- Starting in version 1806, enable a PXE responder on a distribution point without Windows Deployment Service.

For more information, see Install and configure distribution points.

NOTE

When the distribution point transfers content, it transfers using the **Background Intelligent Transfer Service** (BITS) built into the Windows operating system. The distribution point role doesn't require the optional BITS IIS Server Extension feature to be installed because the client does not upload information to it.

System Center Configuration Manager site size and performance guidelines

9/11/2019 • 16 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

System Center Configuration Manager leads the industry in scalability and performance. Other documentation covers maximum supported scalability limits and hardware guidelines for running sites at the largest environment sizes. This article gives supplemental performance guidance for environments of all sizes. This guidance can help you more accurately estimate the hardware you need to deploy Configuration Manager.

This article focuses on the largest contributor to Configuration Manager performance bottlenecks: the disk input/output subsystem or IOPS. The article:

- Presents details and test results focused on IOPS
- Documents how to reproduce the tests with your own environments and hardware
- Suggests disk IOPS requirements for various size environments

Performance test methodology

You can deploy Configuration Manager in many unique ways, but it's important to understand a few variables in any sizing discussions. One variable is *feature interval*, such as an inventory cycle. Another variable is the number of users, software deployments, or other *objects* the system references or deploys. Performance testing applies these variables as part of a *load*. The load generates objects at a typical rate for enterprise customers using production deployments in different size environments.

> **NOTE**
> Customer telemetry data allows for testing current branch builds with the most common scenarios, configurations, and settings for most customers. The recommendations in this article are based on these averages. Your experiences may vary based on your environment size and configuration. In general, Configuration Manager requires common sense when it comes to objects and intervals. Just because you can collect every file on a system, or set the interval for a cycle to one minute, doesn't mean you should.

The following sections highlight some key settings and configurations to use when testing and modeling processing needs for large enterprises. These guidelines help set basic system performance expectations for the suggested hardware sizes.

Feature intervals settings

Most testing should use default intervals for the key cycles in the system. For example, hardware inventory testing occurs once per week with a larger than default *.mof* file. Some recurring feature intervals, especially hardware and software inventory cycles, can have significant effects on an environment's performance characteristics. Environments that enable aggressive default intervals for data collection need oversized hardware in direct proportion to the increase in activity. For example, say you have 25,000 desktop clients and want to collect hardware inventory two times faster than the default interval. You should start by sizing your site's hardware as if you had 50,000 clients.

Objects

Tests should use the *upper average* of the objects that large enterprises tend to use with the system. Typical values are thousands of collections and applications, which are deployed to hundreds of thousands of users or systems.

Tests should run simultaneously on *all* objects in the system at these limits. Many customers leverage several features, but don't generally use all features of the product at these upper limits. Testing with all product features helps ensure the best possible system-wide performance, and allows a buffer for features that some customers may use above average.

Loads

Tests should also run on greater than standard *average day* loads, by performing simulations that generate peak usage demands on the system. One example is simulating Patch Tuesday rollouts, to make sure the system can return update compliance data promptly during these days of peak activity. Another example is simulating site activity during a widespread malware outbreak, to ensure timely notification and response are possible. Although deployed machines of the recommended size may be underused on any given day, more extreme situations require some processing buffer.

Configurations

Run testing on a range of physical, Hyper-V, and Azure hardware, with a mixture of supported operating systems and SQL Server versions. Always validate the worst cases for the supported configuration. In general, Hyper-V and Azure return comparable performance results to equivalent physical hardware when configured similarly. Newer server operating systems tend to perform equally or better than older supported server operating systems. While all supported platforms meet the minimum requirements, usually the latest versions of supporting products like Windows and SQL produce even better performance.

The largest variation comes from the SQL Server versions in use. For more information about SQL Server versions, see What version of SQL should I run?.

Key performance determinants

You can test and measure Configuration Manager performance with a variety of settings, in different ways, and at different site sizes. The following settings and objects can dramatically affect performance. Be sure to consider them when testing and modeling performance in your environment.

Caution

While few aspects of Configuration Manager have official maximums or user interface limits that prevent excessive usage, going beyond the guidelines can have significant adverse effects on a site's performance. Exceeding recommended levels or ignoring sizing guidance typically requires larger hardware, and may render your environment unmaintainable until you reduce the frequency or count of various objects.

Hardware inventory

To test baseline performance, set hardware inventory collection to once per week, with the default *.mof* file size plus approximately 20% additional properties. Don't enable all properties, and collect only properties you actually need. Pay special attention when collecting properties, such as available virtual memory, that will *always* change with *every* inventory cycle. Collecting these properties can cause excessive churn on every inventory cycle from every client.

Software inventory

To test baseline performance, set software inventory collection to once per week, with *product only* details. Collecting many files can place a significant strain on the inventory subsystem. Avoid specifying filters that could end up collecting thousands of files across many clients, such as **.exe* or **.dll*.

Collections

Baseline performance testing can include several thousand collections with a variety of scope, size, complexity, and update settings. Site performance isn't a direct function of the sheer number of collections on a site. Performance is also a cross-product of collections' query complexity, full and incremental updates and change frequency, dependencies among collections, and numbers of clients in the collections.

Where possible, minimize collections that have expensive or complicated dynamic rule queries. For collections that

require these types of rules, set appropriate update intervals and update times to minimize the impact of collection re-evaluation on the system. For example, update at midnight instead of 8:00 AM.

Enabling incremental updates on collections ensures quick and timely updates to collection membership. But even though incremental updates are efficient, they still put load on the system. Balance the change frequency you anticipate with the need for near real-time updates on membership. For example, say you expect heavy churn in collection members, but you don't require near real-time membership updates. It's more efficient and produces less load on the system to update the collection with a scheduled full update at some interval, than to enable incremental updates.

When you enable incremental updates, reduce any scheduled full updates on the same collections. They're only a backup method of evaluation, since incremental updates should keep your collection membership updated in near real time. Best practices for collections recommends a maximum number of total collections for incremental updates, but as the article points out, your experience can vary based on many factors.

Collections with only direct membership rules and with a limiting collection that isn't performing incremental updates don't need scheduled full updates. Disable update schedules for these types of collections to prevent unnecessary load on the system. If the limiting collection uses incremental updates, collections with only direct membership rules may not reflect membership updates for up to 24 hours, or until a scheduled refresh takes place.

While not a best practice, some organizations create hundreds or even thousands of collections as part of various business processes. If you use automation to create collections, it's important to enable any needed incremental updates correctly. Minimize and spread out any full update schedules to avoid hot spots of collection evaluation during a single time period. Establish a regular grooming process to delete unused collections, especially if you automatically create collections that you no longer need after some time.

Remember that Configuration Manager creates policies for all objects in your collections when you target tasks like deployments to them. Membership changes, either through scheduled refresh or incremental updates, can create a lot of other work for the whole system. The latest current branch builds have special policy optimizations for the All Systems and All Users collections. When targeting your entire enterprise, use the built-in collections instead of a clone of these built-in collections.

To investigate collection performance even deeper, you can use the Collection Evaluation Viewer (CEViewer) in the Configuration Manager Toolkit.

Discovery methods

For baseline performance testing, run server-based discovery methods once a week, enabling delta discovery as appropriate to keep the data fresh during the week. The tests should discover an object quantity proportional to the simulated enterprise size. The performance baseline test for heartbeat discovery should also run once a week.

Discovery data is global data. A common performance-related problem is to misconfigure server-based discovery methods in a hierarchy, causing duplicate discovery of the same resources from multiple primary sites. Carefully configure discovery methods to optimize communication with the target service, such as Active Directory domain controllers, while avoiding duplication of the same discovery scope on multiple primary sites.

General sizing guidelines

Based on the preceding performance test methodology, the following table gives general *minimum* hardware requirement guidelines for specific numbers of managed clients. These values should allow most customers with the specified number of clients to process objects fast enough to administer the specified site. Computing power continues to decrease in price every year, and some of the requirements below are small in terms of modern server hardware configurations. Hardware that exceeds the following guidelines proportionally increases performance for sites that require additional processing power, or have special product usage patterns.

DESKTOP CLIENTS	SITE TYPE/ROLE	CORES[1]	MEMORY (GB)	SQL MEMORY ALLOCATION	IOPS: INBOXES[2]	IOPS: SQL[2]	STORAGE SPACE REQUIRED (GB)[3]
25k	Primary or CAS with database site role on the same server	6	24	65%	600	1700	350
25k	Primary or CAS	4	8		600		100
	Remote SQL	4	16	70%		1700	250
50k	Primary or CAS with database site role on the same server	8	32	70%	1200	2800	600
50k	Primary or CAS	4	8		1200		200
	Remote SQL	8	24	70%		2800	400
100k	Primary or CAS with database site role on the same server	12	64	70%	1200	5000	1100
100k	Primary or CAS	6	12		1200		300
	Remote SQL	12	48	80%		5000	800
150k	Primary or CAS with database site role on the same server	16	96	70%	1800	7400	1600
150k	Primary or CAS	8	16		1800		400

DESKTOP CLIENTS	SITE TYPE/ROLE	CORES	MEMORY (GB)	SQL MEMORY ALLOCATION	IOPS: INBOXES	IOPS: SQL	STORAGE SPACE REQUIRED (GB)
	Remote SQL	16	72	90%		7400	1200
700k	CAS with database site role on the same server	20+	128+	80%	1800+	9000+	5000+
700k	CAS	8+	16+		1800+		500+
	Remote SQL	16+	96+	90%		9000+	4500+
5k	Secondary Site	4	8		500	-	200
15k	Secondary Site	8	16		500	-	300

Notes

1. **Cores**: Configuration Manager performs many simultaneous processes, so needs a certain minimum number of CPU cores for various site sizes. While cores get faster each year, it's important to ensure that a certain minimum number of cores work in parallel. In general, any server-level CPU produced after 2015 meets the basic performance needs for the cores specified in the table. Configuration Manager takes advantage of additional cores beyond the recommendations, but generally, once you have the minimum suggested cores, you should prioritize CPU resource investment to increase the speed of existing cores, not add more, slower cores. For example, Configuration Manager will perform better on key processing tasks with 16 fast cores than with 24 slower cores, assuming enough other system resources like disk IOPS are available.

   The relationship between cores and memory is also important. In general, having less than 3-4 GB of RAM per core reduces the total processing capability on your SQL servers. You need more RAM per core when SQL is colocated with the site server components.

   > **NOTE**
   > All testing sets machine power plans to allow maximum CPU power consumption and performance.

2. **IOPS: Inboxes and IOPS: SQL** refer to the IOPS needs for the Configuration Manager and SQL logical drives. The **IOPS: Inboxes** column shows the IOPS requirements for the logical drive where the Configuration Manager inbox directories reside. The **IOPS: SQL** column shows the total IOPS needs for the logical drive(s) that various SQL files use. These columns are different because the two drives should have different formatting. For more information and examples on suggested SQL disk configurations and file best practices, including details on splitting files across multiple volumes, see the Site sizing and performance FAQ.

Both of these IOPS columns use data from the industry-standard tool, *Diskspd*. See How to measure disk performance for instructions on duplicating these measurements. In general, once you meet basic CPU and memory requirements, the storage subsystem has the largest impact on site performance, and improvements here will give the most payback on investment.

3. **Storage space required:** These real-world values may differ from other documented recommendations. We provide these numbers only as a general guideline; individual requirements could vary widely. Carefully plan for disk space needs before site installation. Assume that some amount of this storage remains as free disk space most of the time. You may use this buffer space in a recovery scenario, or for upgrade scenarios that need free disk space for setup package expansion. Your site may require additional storage for large amounts of data collection, longer periods of data retention, and large amounts of software distribution content. You can also store these items on separate, lower-throughput volumes.

How to measure disk performance

You can use the industry-standard tool *Diskspd* to provide standardized suggestions for the IOPS that various-sized Configuration Manager environments require. While not exhaustive, the following test steps and command lines provide a simple and reproducible way to estimate your servers' disk subsystem throughput. You can compare your results to the minimum recommended IOPS in the general sizing guidelines table.

See Example disk configurations for test results from a variety of hardware configurations in lab environments. You can use the data for a rough starting point when designing the storage subsystem for a new environment from scratch.

To test disk IOPS

1. Download the *Diskspd* utility here: https://gallery.technet.microsoft.com/DiskSpd-A-Robust-Storage-6ef84e62.

2. Make sure you have at least 100 GB of free disk space. Disable any apps that might interfere or cause extra load on the disk, such as active antivirus scanning of the directory, SQL, or SMSExec.

3. Run *Diskspd* from an elevated command prompt.

   Perform two runs of the tool in sequence for the volume that you want to test. The first test performs 64k-size, random write operations for one minute. This test ensures controller cache loading and disk space allocation, in case the volume is dynamically expanding. Discard the results of the first test. The second test should *immediately* follow the first test, and perform the same load for five minutes.

   For example, use the following specific command lines to test the G:\ volume.

   ```
   DiskSpd.exe -r -w100 -t8 -o8 -b64K -c100G -d60 -h -L G:\\test\testfile.dat
   ```

   ```
   del G:\\test\testfile.dat
   ```

   ```
   DiskSpd.exe -r -w100 -t8 -o8 -b64K -c100G -d300 -h -L G:\\test\testfile.dat
   ```

4. Review the output from the second test to find the total IOPS in the **I/O per s** column. In the following example, the total IOPS are **3929.18**.

```
Total IO
| thread |  bytes      |  I/Os   |  MB/s  | I/O per s | AvgLat | LatStdDev |
|--------|-------------|---------|--------|-----------|--------|-----------|
|   1    |  9651814400 |  147275 |  30.68 |    490.92 | 16.294 | 10.210    |
|   2    |  9676652544 |  147654 |  30.76 |    492.18 | 16.252 |  9.998    |
|   3    |  9638248448 |  147068 |  30.64 |    490.23 | 16.317 | 10.295    |
|   4    |  9686089728 |  147798 |  30.79 |    492.66 | 16.236 | 10.072    |
|   5    |  9590931456 |  146346 |  30.49 |    487.82 | 16.398 | 10.384    |
|   6    |  9677242368 |  147663 |  30.76 |    492.21 | 16.251 | 10.067    |
|   7    |  9637330944 |  147054 |  30.64 |    490.18 | 16.319 | 10.249    |
|   8    |  9692577792 |  147897 |  30.81 |    492.99 | 16.225 | 10.125    |
| Total: | 77250887680 | 1178755 | 245.57 |   3929.18 | 16.286 | 10.176    |
```

Example disk configurations

The following tables show results from running the test steps in How to measure disk performance with various test lab configurations. Use this data for a *rough* starting point when designing the storage subsystem for a new environment from scratch.

Physical machines and Hyper-V

Hardware is always improving. Expect newer generations of hardware and different hardware combinations, like SSDs and SANs, to exceed the performance stated below. These results are a basic starting point to consider when designing a server or discussing with your hardware vendor.

The following table shows the test results across various disk subsystems, including spindle and SSD-based hard drives, in various test lab configurations. All configurations format the disks with 64k clusters and attach them to an enterprise class disk controller. In addition to the RAID array disk count, they each have at least one spare disk.

DISK TYPE	DISK COUNT, NOT INCLUDING +1 SPARE DISK	RAID	IOPS MEASURED
15k SAS	2	1	620
15k SAS	4	10	1206
15k SAS	6	10	1751
15k SAS	8	10	2322
15k SAS	10	10	2882
15k SAS	12	10	3476
15k SAS	16	10	4236
15k SAS	20	10	5148
15k SAS	30	10	7398
15k SAS	40	10	9913
SSD SATA	2	1	3300
SSD SATA	4	10	5542

DISK TYPE	DISK COUNT, NOT INCLUDING +1 SPARE DISK	RAID	IOPS MEASURED
SSD SATA	6	10	7201
SSD SAS	2	1	7539
SSD SAS	4	10	14346
SSD SAS	6	10	15607

These are the devices the example used. This information isn't a recommendation for any specific hardware model or manufacturer.

DISK TYPE	MODEL	RAID CONTROLLER	CACHE MEMORY AND CONFIGURATION
15k RPM SAS HD	HP EH0300JDYTH	Smart Array P822	2GB, 20% Read / 80% Write
SSD SATA	ATA MK0200GCTYV	Smart Array P420i	1GB, 20% Read / 80% Write
SSD SAS	HP MO0800 JEFPB	Smart Array P420i	1GB, 20% Read / 80% Write

Azure machine and disk performance

Azure disk performance depends on several factors, such as the size of the Azure VM, and the number and type of disks it uses. Azure is also constantly adding new machine types and disk speeds that are different from the following chart. For more information about Configuration Manager running on Azure, and additional information on understanding disk I/O on Azure, see Configuration Manager on Azure frequently asked questions.

All disks are formatted NTFS 64k cluster size, and rows with more than one disk are configured as striped volumes via the Windows Disk Management utility.

AZURE VM	AZURE DISK	DISK COUNT	AVAILABLE SPACE	IOPS MEASURED	LIMITING FACTOR
DS2/DS11	P20	1	512 MB	965	Azure VM size
DS2/DS11	P20	2	1024 MB	996	Azure VM size
DS2/DS11	P30	1	1024 MB	996	Azure VM size
DS2/DS11	P30	2	2048 MB	996	Azure VM size
DS3/DS12/F4S	P20	1	512 MB	1994	Azure VM size
DS3/DS12/F4S	P20	2	1024 MB	1992	Azure VM size
DS3/DS12/F4S	P30	1	1024 MB	1993	Azure VM size
DS3/DS12/F4S	P30	2	2048 MB	1992	Azure VM size
DS4/DS13/F8S	P20	1	512 MB	2334	P20 disk
DS4/DS13/F8S	P20	2	1024 MB	3984	Azure VM size

AZURE VM	AZURE DISK	DISK COUNT	AVAILABLE SPACE	IOPS MEASURED	LIMITING FACTOR
DS4/DS13/F8S	P20	3	1536 MB	3984	Azure VM size
DS4/DS13/F8S	P30	1	1024 MB	3112	P30 disk
DS4/DS13/F8S	P30	2	2048 MB	3984	Azure VM size
DS4/DS13/F8S	P30	3	3072 MB	3996	Azure VM size
DS5/DS14/F16S	P20	1	512 MB	2335	P20 disk
DS5/DS14/F16S	P20	2	1024 MB	4639	P20 disk
DS5/DS14/F16S	P20	3	1536 MB	6913	P20 disk
DS5/DS14/F16S	P20	4	2048 MB	7966	Azure VM size
DS5/DS14/F16S	P30	1	1024 MB	3112	P30 disk
DS5/DS14/F16S	P30	2	2048 MB	6182	P30 disk
DS5/DS14/F16S	P30	3	3072 MB	7963	Azure VM size
DS5/DS14/F16S	P30	4	4096 MB	7968	Azure VM size
DS15	P30	1	1024 MB	3113	P30 disk
DS15	P30	2	2048 MB	6184	P30 disk
DS15	P30	3	3072 MB	9225	P30 disk
DS15	P30	4	4096 MB	10200	Azure VM size

See also

- Site sizing and performance FAQ
- Configuration Manager on Azure frequently asked questions
- Size and scale numbers
- Recommended hardware

Supported operating systems for Configuration Manager site system servers

6/19/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article details the Windows versions that you can use to host a Configuration Manager site or site system role.

Use the information in this article with the information in the following articles:

- Recommended hardware for Configuration Manager
- Site and site system prerequisites for Configuration Manager
- Size and scale numbers for Configuration Manager

Windows Server 2019

Applies to Windows Server 2019: Standard and Datacenter

Starting in version 1810, this OS version is supported for the following roles:

Site servers

- Central administration site
- Primary site
- Secondary site

Site system servers

- Application Catalog web service point
- Application Catalog website point
- Asset Intelligence synchronization point
- Certificate registration point
- Cloud management gateway connection point
- Data warehouse service point
- Distribution point [Note 1]
- Endpoint Protection point
- Enrollment point
- Enrollment proxy point
- Fallback status point
- Management point
- Reporting services point
- Service connection point
- Site database server [Note 2]
- SMS_Provider
- Software update point
- State migration point

Windows Server 2016

Applies to Windows Server 2016: Standard and Datacenter

This OS version is supported for the following roles:

Site servers

- Central administration site
- Primary site
- Secondary site

Site system servers

- Application Catalog web service point
- Application Catalog website point
- Asset Intelligence synchronization point
- Certificate registration point
- Cloud management gateway connection point
- Data warehouse service point
- Distribution point [Note 1]
- Endpoint Protection point
- Enrollment point
- Enrollment proxy point
- Fallback status point
- Management point
- Reporting services point
- Service connection point
- Site database server [Note 2]
- SMS_Provider
- Software update point
- State migration point

Windows Storage Server 2016

Site system server

- Distribution point [Note 1]

Windows Server 2012 R2

Applies to Windows Server 2012 R2: Standard and Datacenter

Site servers

- Central administration site
- Primary site
- Secondary site

Site system servers

- Application Catalog web service point
- Application Catalog website point
- Asset Intelligence synchronization point
- Certificate registration point
- Cloud management gateway connection point
- Data warehouse service point
- Distribution point [Note 1]
- Endpoint Protection point
- Enrollment point

- Enrollment proxy point
- Fallback status point
- Management point
- Reporting services point
- Service connection point
- Site database server [Note 2]
- SMS_Provider
- Software update point
- State migration point

Windows Server 2012

Applies to Windows Server 2012: Standard and Datacenter

Site servers

- Central administration site
- Primary site
- Secondary site

Site system servers

- Application Catalog web service point
- Application Catalog website point
- Asset Intelligence synchronization point
- Certificate registration point
- Cloud management gateway connection point
- Data warehouse service point
- Distribution point [Note 1]
- Endpoint Protection point
- Enrollment point
- Enrollment proxy point
- Fallback status point
- Management point
- Reporting services point
- Service connection point
- Site database server [Note 2]
- SMS_Provider
- Software update point
- State migration point

Windows Server 2008 R2 with SP1

Applies to Windows Server 2008 R2 with Service Pack 1: Standard, Enterprise, and Datacenter

Windows Server 2008 R2 is now in extended support and no longer in mainstream support, as detailed in Microsoft Support Lifecycle. For more information about future support for these operating systems as site system servers with Configuration Manager, see Deprecated server operating systems.

> **IMPORTANT**
> The extended support end date for Windows Server 2008 R2 is January 14, 2020. After this date, Configuration Manager won't support this OS as any site system role.

This OS isn't supported for site servers or most site system roles. It's still supported for the distribution point site system role, including pull-distribution points and for PXE and multicast.

Site system servers

- Distribution point [Note 1]
  - Distribution points on this OS support PXE and multicast.

Windows Server 2008 with SP2

Applies to Windows Server 2008 with Service Pack 2 (x86, x64): Standard, Enterprise, and Datacenter

Windows Server 2008 with Service Pack 2 (SP2) is now in extended support and no longer in mainstream support, as detailed in Microsoft Support Lifecycle. For more information about future support for these operating systems as site system servers with Configuration Manager, see Deprecated server operating systems.

> **IMPORTANT**
> The extended support end date for Windows Server 2008 R2 is January 14, 2020. After this date, Configuration Manager won't support this OS as any site system role.

This OS isn't supported for site servers or site system roles, except for the distribution point and pull-distribution point. Continue to use this OS as a distribution point until deprecation of this support is announced, or this OS's extended support period expires. For more information, see Installation of Configuration Manager CB and LTSB fails on Windows Server 2008.

Site system servers

- Distribution point [Note 1]
  - Distribution points on this OS support PXE and multicast.
  - Distribution points on this OS don't support network booting of client computers in EFI mode. Client computers with BIOS or with EFI booting in legacy mode are supported.

> **WARNING**
> Windows Server 2008 doesn't support TLS 1.2. If you enable this protocol in your environment, Windows Server 2008 computers will no longer communicate with the site. For more information, see How to enable TLS 1.2 for Configuration Manager.

Client OS versions

The following client OS versions are supported for use as a **distribution point** [Note 1]:

- Windows 10 (x86, x64): Pro and Enterprise
- Windows 8.1 (x86, x64): Professional and Enterprise
- Windows 7 with SP1 (x86, x64): Professional, Enterprise, and Ultimate

This support has the following limitation:

- Distribution points on this OS don't support PXE or multicast with the default Windows Deployment Services. Starting in version 1806, you can PXE-enable a distribution point on this OS with the option to **Enable a PXE responder without Windows Deployment Service**. For more information, see Install and configure distribution points.

Server core installations

The server core installation of the following server OS versions are supported for use as a **distribution point**:

- Windows Server 2019 (starting in Configuration Manager, version 1810)
- Windows Server, version 1809 (starting in Configuration Manager, version 1810)
- Windows Server, version 1803 (starting in Configuration Manager, version 1802)
- Windows Server, version 1709 (starting in Configuration Manager, version 1710)
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

This support has the following limitation:

- Distribution points on this OS don't support PXE or multicast with the default Windows Deployment Services. Starting in version 1806, you can PXE-enable a distribution point on this OS with the option to **Enable a PXE responder without Windows Deployment Service**. For more information, see Install and configure distribution points.

General notes

Note 1: Distribution points

Distribution points support several different configurations that each have different requirements. In some cases, these configurations support installation not only on servers, but on client operating systems. For more information, see Manage content and content infrastructure.

Note 2: Site database servers

Site database servers aren't supported on a read-only domain controller (RODC). For more information, see the Microsoft Support article: You may encounter problems when installing SQL Server on a domain controller.

Additionally, secondary site servers aren't supported on any domain controller.

Supported OS versions for clients and devices for Configuration Manager

9/5/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager supports installing client software on Windows and macOS computers.

General requirements and limitations

Review the following requirements and limitations for all clients:

- Changing the startup type or **Log on as** settings for any Configuration Manager service isn't supported. This change can prevent key services from running correctly.

Windows computers

To manage the following Windows OS versions, use the client that's included with Configuration Manager. For more information, see How to deploy clients to Windows computers.

Supported client OS versions

- **Windows 10**

  For more detailed information, see Support for Windows 10.

- **Windows 8.1** (x86, x64): Professional, Enterprise
- **Windows 7 with SP1** (x86, x64): Professional, Enterprise, and Ultimate

Windows Virtual Desktop

Windows Virtual Desktop is a preview feature of Microsoft Azure and Microsoft 365. Starting in version 1906, use Configuration Manager to manage these virtual devices running Windows in Azure.

Similar to a terminal server, these virtual devices allow multiple concurrent active user sessions. To help with client performance, Configuration Manager now disables user policies on any device that allows these multiple user sessions. Even if you enable user policies, the client disables them by default on these devices, which include Windows Virtual Desktop and terminal servers.

The client only disables user policy when it detects this type of device during a new installation. For an existing client of this type that you update to this version, the previous behavior persists. On an existing device, it configures the user policy setting even if it detects that the device allows multiple user sessions.

If you require user policy in this scenario, and accept any potential performance impact, use the Configuration Manager SDK with the SMS_PolicyAgentConfig server WMI class. Set the new `PolicyEnableUserPolicyOnTS` property to `true`.

> **NOTE**
> You can't use co-management with a Windows Virtual Desktop. Windows 10 Enterprise for Virtual Desktop (EVD) is actually a Windows Server edition, which doesn't have the MDM components.

Supported server OS versions

- **Windows Server 2019**: Standard, Datacenter [Note 1]
  (Starting with Configuration Manager version 1806.)
- **Windows Server 2016**: Standard, Datacenter [Note 1]
- **Windows Storage Server 2016**: Workgroup, Standard
- **Windows Server 2012 R2** (x64): Standard, Datacenter [Note 1]
- **Windows Storage Server 2012 R2** (x64)
- **Windows Server 2012** (x64): Standard, Datacenter [Note 1]
- **Windows Storage Server 2012** (x64)
- **Windows Server 2008 R2 with SP1** (x64): Standard, Enterprise, Datacenter [Note 1]
- **Windows Storage Server 2008 R2** (x86, x64): Workgroup, Standard, Enterprise
- **Windows Server 2008 with SP2** (x86, x64): Standard, Enterprise, Datacenter [Note 1]

Server Core

The following versions specifically refer to the Server Core installation of the OS. [Note 3]

Windows Server semi-annual channel versions are Server Core installations, such as Windows Server, version 1809. As a Configuration Manager client, they're supported the same as the associated Windows 10 semi-annual channel version. For more information, see Support for Windows 10.

- **Windows Server 2019** (x64) [Note 2]
- **Windows Server 2016** (x64) [Note 2]
- **Windows Server 2012 R2** (x64) [Note 2]
- **Windows Server 2012** (x64) [Note 2]
- **Windows Server 2008 R2** with no service pack, or with SP1 (x64)
- **Windows Server 2008 SP2** (x86, x64)

Note 1

Configuration Manager tests and supports Windows Server Datacenter editions, but isn't officially certified for Windows Server. Configuration Manager hotfix support isn't offered for issues that are specific to Windows Server Datacenter Edition. For more information on the Windows Server certification program, see Windows Server Catalog.

Note 2

To support client push installation, add the File Server service of the File and Storage Services server role. For more information about installing Windows features on Server Core, see Install roles, role services, and features by using Windows PowerShell cmdlets.

Note 3

The new Software Center app isn't supported on any version of Windows Server Core.

Windows Embedded computers

Manage Windows Embedded devices by installing the Configuration Manager client on the device. For more information, see Planning for client deployment to Windows Embedded devices.

Requirements and limitations

- All client features are supported on Windows Embedded systems that don't have write filters enabled.

- Clients that use one of the following are supported for all features except power management:
  - Enhanced Write Filters (EWF)
  - RAM File-Based Write Filters (FBWF)
  - Unified Write Filters (UWF)
- The application catalog isn't supported for any Windows Embedded device.

Supported OS versions

- **Windows 10 Enterprise** (x86, x64)
- **Windows 10 IoT Enterprise** (x86, x64)
  This version includes the long-term servicing channel (LTSC). For more information, see Overview of Windows 10 IoT Enterprise.
- **Windows Embedded 8.1 Industry** (x86, x64)
- **Windows Embedded 8 Standard** (x86, x64)
- **Windows Thin PC** (x86, x64)
- **Windows Embedded POSReady 7** (x86, x64)
- **Windows Embedded Standard 7 with SP1** (x86, x64)

Windows CE computers

Manage Windows CE devices with the Configuration Manager mobile device legacy client that is included with Configuration Manager.

Requirements and limitations

- The mobile device client requires 0.78 MB of storage space for installation. Sign-in can require up to 256 KB of additional storage space.
- Features for these mobile devices vary by platform and client type. For information about which management functions are supported, see Choose a device management solution.

Supported OS versions

- Windows CE 7.0 (ARM and x86 processors)

> **NOTE**
> Support is deprecated for Windows CE 7.0 in Configuration Manager. For more information, see Removed and deprecated items for Configuration Manager clients.

Supported languages include

- Chinese (simplified and traditional)
- English (US)
- French (France)
- German
- Italian
- Japanese

- Korean
- Portuguese (Brazil)
- Russian
- Spanish (Spain)

Mac computers

Manage Apple Mac computers with the Configuration Manager client for macOS.

The macOS client installation package isn't supplied with the Configuration Manager media. Download the **Clients for Additional Operating Systems** from the Microsoft Download Center.

For more information, see How to deploy clients to Macs.

Requirements and limitations

- Installing or running the Configuration Manager client for macOS on computers under an account other than root isn't supported. Doing so can prevent key services from running correctly.

Supported versions

- **macOS Mojave (10.14)**
- **macOS High Sierra (10.13)**
- **macOS Sierra (10.12)**
- **macOS 10.11** (El Capitan)
- **macOS 10.10** (Yosemite)
- **macOS 10.9** (Mavericks)
- **macOS 10.8** (Mountain Lion)
- **macOS 10.7** (Lion)
- **macOS 10.6** (Snow Leopard)

Linux and UNIX servers

> **IMPORTANT**
> Configuration Manager version 1902 drops support for Linux and UNIX as a client. Deprecation was announced with version 1802. Consider Microsoft Azure Management for managing Linux servers. Azure solutions have extensive Linux support that in most cases exceed Configuration Manager functionality, including end-to-end patch management for Linux.

The Linux and UNIX client installation packages aren't supplied with the Configuration Manager media. Download the **Clients for Additional Operating Systems** from the Microsoft Download Center. In addition to client installation packages, the client download includes the script that manages the installation of the client on each computer.

Requirements and limitations

- To review OS file dependencies for the client for Linux and UNIX, see Prerequisites for client deployment to Linux and UNIX servers.
- For an overview of supported management capabilities for Linux or UNIX, see How to deploy clients to UNIX and Linux servers.

- For supported versions of Linux and UNIX, the listed version includes all subsequent minor versions. For example, CentOS version 6 includes CentOS 6.3. Similarly, support for an OS that uses service packs (such as SUSE Linux Enterprise Server 11 SP1) includes subsequent service packs for that OS version.
- For information about client installation packages and the Universal Agent, see How to deploy clients to UNIX and Linux servers.

Supported versions

The following versions are supported by using the indicated .tar file.

AIX

VERSION	TAR FILE
Version 6.1 (Power)	ccm-Aix61ppc.<build>.tar
Version 7.1 (Power)	ccm-Aix71ppc.<build>.tar

CentOS

VERSION	TAR FILE
Version 5 x86	ccm-Universalx86.<build>.tar
Version 5 x64	ccm-Universalx64.<build>.tar
Version 6 x86	ccm-Universalx86.<build>.tar
Version 6 x64	ccm-Universalx64.<build>.tar
Version 7 x64	ccm-Universalx64.<build>.tar

Debian

VERSION	TAR FILE
Version 5 x86	ccm-Universalx86.<build>.tar
Version 5 x64	ccm-Universalx64.<build>.tar
Version 6 x86	ccm-Universalx86.<build>.tar
Version 6 x64	ccm-Universalx64.<build>.tar
Version 7 x86	ccm-Universalx86.<build>.tar
Version 7 x64	ccm-Universalx64.<build>.tar
Version 8 x86	ccm-Universalx86.<build>.tar
Version 8 x64	ccm-Universalx64.<build>.tar

HP-UX

VERSION	TAR FILE
Version 11iv3 IA64	ccm-HpuxB.11.31i64.<build>.tar

Oracle Linux

VERSION	TAR FILE
Version 5 x86	ccm-Universalx86.<build>.tar
Version 5 x64	ccm-Universalx64.<build>.tar
Version 6 x86	ccm-Universalx86.<build>.tar
Version 6 x64	ccm-Universalx64.<build>.tar
Version 7 x64	ccm-Universalx64.<build>.tar

Red Hat Enterprise Linux (RHEL)

VERSION	TAR FILE
Version 5 x86	ccm-Universalx86.<build>.tar
Version 5 x64	ccm-Universalx64.<build>.tar
Version 6 x86	ccm-Universalx86.<build>.tar
Version 6 x64	ccm-Universalx64.<build>.tar
Version 7 x64	ccm-Universalx64.<build>.tar

Solaris

VERSION	TAR FILE
Version 10 x86	ccm-Sol10x86.<build>.tar
Version 10 SPARC	ccm-Sol10sparc.<build>.tar
Version 11 x86	ccm-Sol11x86.<build>.tar
Version 11 SPARC	ccm-Sol11sparc.<build>.tar

SUSE Linux Enterprise Server (SLES)

VERSION	TAR FILE
Version 10 SP1 x86	ccm-Universalx86.<build>.tar
Version 10 SP1 x64	ccm-Universalx64.<build>.tar
Version 11 SP1 x86	ccm-Universalx86.<build>.tar

VERSION	TAR FILE
Version 11 SP1 x64	ccm-Universalx64.<build>.tar
Version 12 x64	ccm-Universalx64.<build>.tar

Ubuntu

VERSION	TAR FILE
Version 10.04 LTS x86	ccm-Universalx86.<build>.tar
Version 10.04 LTS x64	ccm-Universalx64.<build>.tar
Version 12.04 LTS x86	ccm-Universalx86.<build>.tar
Version 12.04 LTS x64	ccm-Universalx64.<build>.tar
Version 14.04 LTS x86	ccm-Universalx86.<build>.tar
Version 14.04 LTS x64	ccm-Universalx64.<build>.tar
Version 16.04 LTS x86	ccm-Universalx86.<build>.tar
Version 16.04 LTS x64	ccm-Universalx64.<build>.tar

On-premises MDM

Configuration Manager has built-in capabilities for managing mobile devices that are on-premises without installing client software. For more information, see Manage mobile devices with on-premises infrastructure.

Requirements and limitations

- Configure the **Service connection point** at the top-tier site of your hierarchy.

Supported operating systems

- **Windows 10 Pro** (x86, x64)
- **Windows 10 Pro Enterprise** (x86, x64)
- **Windows 10 IoT Enterprise** (x86, x64)
  This version includes the long-term servicing channel (LTSC). For more information, see Overview of Windows 10 IoT Enterprise.
- **Windows 10 IoT Mobile Enterprise**
- **Windows 10 Team for Surface Hub**
- **Windows 10 Mobile**
- **Windows 10 Mobile Enterprise**

> **NOTE**
> Support is deprecated for Windows 10 Mobile and Windows 10 Mobile Enterprise in Configuration Manager. For more information, see Removed and deprecated items for Configuration Manager clients.

Exchange Server connector

Configuration Manager supports limited management of devices that connect to your Exchange Server, without installing the Configuration Manager client. For more information, see Manage mobile devices with Configuration Manager and Exchange.

Supported versions of Exchange Server

- **Exchange Online (Office 365)**: This version includes Business Productivity Online Standard Suite
- **Exchange Server 2016**
- **Exchange Server 2013**
- **Exchange Server 2010 SP1** or **Exchange Server 2010 SP2**

Support for Windows 10 in Configuration Manager

9/6/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Learn about the Windows 10 versions that Configuration Manager supports, including:

- Windows 10 as a Configuration Manager client
- The Windows Assessment and Deployment Kit (ADK) for Windows 10

> **TIP**
> Windows Server builds as a client are supported the same as the associated Windows 10 version. For example, Windows Server 2016 is the same build version as Windows 10 LTSB 2016, and Windows Server version 1803 is the same build version as Windows 10 version 1803.
>
> For more information on Windows Server as a site system, see Supported operating systems for Configuration Manager site system servers.

Windows 10 as a client

Configuration Manager attempts to provide support as a client for each new Windows 10 version as soon as possible after it becomes available. Because the products have separate development and release schedules, the support that Configuration Manager provides depends on when each becomes available.

A Configuration Manager version drops from the matrix after support for that version ends. Similarly, support for Windows 10 versions like the Enterprise 2015 LTSB or 1511 drops from the matrix when they're removed from support.

- The latest version of Configuration Manager current branch receives both security and critical updates, which can include fixes for issues with Windows 10 versions. When Microsoft releases a new version of Configuration Manager current branch, prior versions only receive security updates. For more information, see Support for Configuration Manager current branch versions.

  > **NOTE**
  > The best way to stay current with Windows 10 is to stay current with Configuration Manager. For more information, see Configuration Manager and Windows as a Service.

- This information supplements Supported operating systems for clients and devices.
- If you use the long-term servicing branch of Configuration Manager, see Supported configurations for the long-term servicing branch.

The following table lists the versions of Windows 10 that you can use as a client with different versions of Configuration Manager.

WINDOWS 10 VERSION	CONFIGURATION MANAGER 1802	CONFIGURATION MANAGER 1806	CONFIGURATION MANAGER 1810	CONFIGURATION MANAGER 1902	CONFIGURATION MANAGER 1906
Enterprise 2015 LTSB	✓	✓	✓	✓	✓
Enterprise 2016 LTSB	✓	✓	✓	✓	✓
Enterprise LTSC 2019	✗	✓	✓	✓	✓
1703	✓	✓	✓	✓	✓
1709	✓	✓	✓	✓	✓
1803	✓	✓	✓	✓	✓
1809	✗	✓	✓	✓	✓
1903	✗	✗	✗	✓	✓

For more information on Windows lifecycle, see the Windows lifecycle fact sheet

NOTE

Support for Windows 10 semi-annual channel versions includes the following editions: Enterprise, Pro, Education, and Pro Education.

Starting in version 1906, Configuration Manager supports Windows 10 Pro for Workstation.

KEY
✓ = **Supported**
✗ = **Not supported**

NOTE

Configuration Manager supports the client on Windows 10 ARM64 devices. Existing client management features should work with these new devices. For example, hardware and software inventory, software updates, and application management. OS deployment is currently not supported.

Windows 10 ADK

When you deploy operating systems with Configuration Manager, the Windows ADK is a required external dependency. For more information, see Infrastructure requirements for OS deployment.

IMPORTANT

Starting with Windows 10 version 1809, Windows PE is a separate installer. Otherwise there's no functional difference.

The following table lists the versions of the Windows 10 ADK that you can use with different versions of Configuration Manager.

WINDOWS 10 ADK VERSION	CONFIGURATION MANAGER 1802	CONFIGURATION MANAGER 1806	CONFIGURATION MANAGER 1810	CONFIGURATION MANAGER 1902	CONFIGURATION MANAGER 1906
1703 (10.1.15063)	BC	✗	✗	✗	✗
1709 (10.1.16299)	✓	BC	✗	✗	✗
1803 (10.1.17134)	✓	✓	BC	BC	✗
1809 (10.1.17763)	✗	✓	✓	✓	BC
1903 (10.1.18362)	✗	✗	✗	✓	✓

> **NOTE**
> Configuration Manager only supports x86 and amd64 components of the Windows 10 ADK. It doesn't currently support ARM or ARM64 components.

KEY

✓ = **Supported**
This table only shows Windows ADK supportability in relation to the version of Configuration Manager. Microsoft recommends using the Windows ADK that matches the version of Windows you're deploying. Use the latest Windows ADK version when deploying the latest Windows 10 version. The latest Windows ADK version may support deployment of older OS versions, such as Windows 7. For more information on Windows ADK component supportability, see DISM supported platforms and USMT requirements.

BC = **Backward compatible**
This combination isn't tested but should work. We'll document any known issues or caveats.

✗ = **Not supported**

> **TIP**
> Windows Server builds have the same Windows ADK requirement as the associated Windows 10 version. For example, Windows Server 2016 is the same build version as Windows 10 LTSB 2016.

Supported OS versions for Configuration Manager consoles

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To support the Configuration Manager console, the following OS versions require a minimum .NET Framework version of 4.5.2. The exception is Windows 10, which requires a minimum of .NET Framework 4.6.

- **Windows Server 2019**: Standard, Datacenter (starting in version 1810)
- **Windows Server 2016**: Standard, Datacenter
- **Windows Server 2012 R2** (x64): Standard, Datacenter
- **Windows Server 2012** (x64): Standard, Datacenter
- **Windows Server 2008 R2 with SP1** (x64): Standard, Enterprise, Datacenter
- **Windows 10** (x86, x64): Pro, Enterprise
- **Windows 8.1** (x86, x64): Professional, Enterprise
- **Windows 7 with SP1** (x86, x64): Professional, Enterprise, Ultimate

For more information about the Configuration Manager console, see the following articles:

- Install consoles
- Using the console

Recommended hardware for System Center Configuration Manager

7/26/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The following recommendations are guidelines to help you scale your System Center Configuration Manager environment to support more than a very basic deployment of sites, site systems, and clients. They are not intended to cover all possible site and hierarchy configurations.

Use the information in the following sections as a guide to help you plan for hardware that can meet the processing loads for clients and sites that use the available Configuration Manager features with the default configurations.

Site systems

This section provides recommended hardware configurations for Configuration Manager site systems for deployments that support the maximum number of clients and use most or all Configuration Manager features. Deployments that support less than the maximum number of clients and don't use all available features might require fewer computer resources. In general, the key factors that limit performance of the overall system include the following, in order:

1. Disk I/O performance
2. Available memory
3. CPU

For best performance, use RAID 10 configurations for all data drives and a 1-Gbps Ethernet network.

Site servers

SITE CONFIGURATION	CPU (CORES)	MEMORY (GB)	MEMORY ALLOCATION FOR SQL SERVER (%)
Stand-alone primary site server with a database site role on the same server[1]	16	96	80
Stand-alone primary site server with a remote site database	8	16	-
Remote database server for a stand-alone primary site	16	72	90
Central administration site server with a database site role on the same server[1]	20	128	80
Central administration site server with a remote site database	8	16	-

SITE CONFIGURATION	CPU (CORES)	MEMORY (GB)	MEMORY ALLOCATION FOR SQL SERVER (%)
Remote database server for a central administration site	16	96	90
Child primary site with a database site role on the same server	16	96	80
Child primary site server with a remote site database	8	16	-
Remote database server for a child primary site	16	72	90
Secondary site server	8	16	-

[1] When the site server and SQL Server are installed on the same computer, the deployment supports the maximum sizing and scale numbers for sites and clients. But, this configuration can limit high availability options for System Center Configuration Manager, like using a SQL Server cluster. Also, because of the higher I/O requirements that are needed to support both SQL Server and the Configuration Manager site server when you're running both on the same computer, it's a good idea to consider using a configuration with a remote SQL Server machine if you have a larger deployment.

Remote site system servers

The following guidance is for computers that hold a single site system role. Plan to make adjustments when you install multiple site system roles on the same computer.

SITE SYSTEM ROLE	CPU (CORES)	MEMORY (GB)	DISK SPACE (GB)
Management point	4	8	50
Distribution point	2	8	As required by the operating system and to store content that you deploy
Software update point[1]	8	16	As required by the operating system and to store updates that you deploy
All other site system roles	4	8	50

[1] The computer that hosts a software update point requires the following configurations for IIS application pools:

- Increase the **WsusPool Queue Length** to **2000**.
- Increase the **WsusPool Private Memory limit** by four times, or set it to **0** (unlimited).

Disk space for site systems

Disk allocation and configuration contributes to the performance of Configuration Manager. Because each Configuration Manager environment is different, the values that you implement can vary from the following guidance.

For the best performance, place each object on a separate, dedicated RAID volume. For all data volumes (Configuration Manager and its database files), use RAID 10 for the best performance.

DATA USAGE	MINIMUM DISK SPACE	25,000 CLIENTS	50,000 CLIENTS	100,000 CLIENTS	150,000 CLIENTS	700,000 CLIENTS (CENTRAL ADMINISTRATION SITE)
Operating system	See guidance for the operating system.	See guidance for the operating system.	See guidance for the operating system.	See guidance for the operating system.	See guidance for the operating system.	See guidance for the operating system.
Configuration Manager application and log files	25 GB	50 GB	100 GB	200 GB	300 GB	200 GB
Site database .mdf file	75 GB for every 25,000 clients	75 GB	150 GB	300 GB	500 GB	2 TB
Site database .ldf file	25 GB for every 25,000 clients	25 GB	50 GB	100 GB	150 GB	100 GB
Temp database files (.mdf and .ldf)	As needed	As needed	As needed	As needed	As needed	As needed
Content (distribution point shares)	As needed[1]	As needed[1]	As needed[1]	As needed[1]	As needed[1]	As needed[1]

[1] The disk space guidance doesn't include the space required for content that is located in the content library on the site server or distribution points. For information about planning for the content library, see The content library.

In addition to the preceding guidance, consider the following guidelines when you plan for disk space requirements:

- Each client requires approximately 5 MB of space.
- When you plan for the size of the Temp database for a primary site, plan for a combined size that is 25% to 30% of the site database .mdf file. The actual size can be significantly smaller or larger—it depends on the performance of the site server and the volume of incoming data over both short and long periods of time.

  > **NOTE**
  > When you have 50,000 or more clients at a site, plan to use four or more Temp database .mdf files.

- The Temp database size for a central administration site is typically much smaller than for a primary site.
- The secondary site database has the following size limitations:
  - SQL Server 2012 Express: 10 GB
  - SQL Server 2014 Express: 10 GB

Clients

This section provides recommended hardware configurations for computers that you manage by using Configuration Manager client software.

Client for Windows computers

The following are minimum requirements for Windows-based computers that you manage by using Configuration Manager, including embedded operating systems:

- **Processor and memory:** Refer to the processor and RAM requirements for the computer operating system.
- **Disk space:** 500 MB available disk space, with 5 GB recommended for the Configuration Manager client cache. Less disk space is required if you use customized settings to install the Configuration Manager client:
  - Use the Client.msi property SMSCACHESIZE to set a cache file that is smaller than the default of 5120 MB. The minimum size is 1 MB. For example, `CCMSetup.exe SMSCachesize=2` creates a cache that is 2 MB in size.

  For more information about these client installation settings, see About client installation properties.

  > **TIP**
  > Installing the client with minimal disk space is useful for Windows Embedded devices that typically have smaller disk sizes than standard Windows computers.

The following are additional minimum hardware requirements for optional functionality in Configuration Manager.

- **Operating system deployment:** 384 MB of RAM
- **Software Center:** 500 MHz processor
- **Remote Control:** Pentium 4 Hyper-Threaded 3 GHz (single core) or comparable CPU, with at least a 1 GB RAM for optimal experience

Client for Linux and UNIX

The following are minimum requirements for Linux and UNIX servers that you manage with Configuration Manager.

REQUIREMENT	DETAILS
Processor and memory	Refer to the processor and RAM requirements for the computer's operating system.
Disk space	500 MB available disk space, with 5 GB recommended for the Configuration Manager client cache.
Network connectivity	Configuration Manager client computers must have network connectivity to Configuration Manager site systems to enable management.

Configuration Manager console

The requirements in the following table apply to each computer that runs the Configuration Manager console.

Minimum hardware configuration:

- Intel i3 or comparable CPU
- 2 GB of RAM
- 2 GB of disk space

DPI SETTING	MINIMUM RESOLUTION
96 / 100%	1024 x 768
120 /125%	1280 x 960
144 / 150%	1600 x 1200
196 / 200%	2500 x 1600

Support for PowerShell:

When you install support for PowerShell on a computer that runs the Configuration Manager console, you can run PowerShell cmdlets on that computer to manage Configuration Manager.

- PowerShell 3.0 or later is supported

In addition to PowerShell, Windows Management Framework (WMF) version 3.0 or later is supported.

Lab deployments

Use the following minimum hardware recommendations for lab and test deployments of Configuration Manager. These recommendations apply to all site types, up to 100 clients:

ROLE	CPU (CORES)	MEMORY (GB)	DISK SPACE (GB)
Site and database server	2 - 4	8 - 12	100
Site system server	1 - 4	2 - 4	50
Client	1 - 2	1 - 3	30

Supported SQL Server versions for Configuration Manager

8/6/2019 • 9 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Each System Center Configuration Manager site requires a supported SQL Server version and configuration to host the site database.

SQL Server instances and locations

Central administration site and primary sites

The site database must use a full installation of SQL Server.

SQL Server can be located on:

- The site server computer.
- A computer that is remote from the site server.

The following instances are supported:

- The default or named instance of SQL Server.
- Multiple instance configurations.
- A SQL Server cluster. See Use a SQL Server cluster to host the site database.
- A SQL Server AlwaysOn availability group. For more information, see SQL Server AlwaysOn for a highly available site database.

Secondary sites

The site database can use the default instance of a full installation of SQL Server or SQL Server Express.

SQL Server must be located on the site server computer.

Limitations to support

The following configurations aren't supported:

- A SQL Server cluster in a Network Load Balancing (NLB) cluster configuration
- A SQL Server cluster on a Cluster Shared Volume (CSV)
- SQL Server database mirroring technology, and peer-to-peer replication

SQL Server transactional replication is supported only for replicating objects to management points that are configured to use database replicas.

Supported versions of SQL Server

In a hierarchy with multiple sites, different sites can use different versions of SQL Server to host the site database. So long as the following items are true:

- Configuration Manager supports the versions of SQL Server that you use.
- The SQL Server versions you use remain in support by Microsoft.
- SQL Server supports replication between the two versions of SQL Server. For more information, see SQL Server replication backward compatibility.

For SQL Server 2016 and prior, support for each SQL version and service pack follows the Microsoft Lifecycle Policy. Support for a specific SQL Server service pack includes cumulative updates unless they break backward compatibility to the base service pack version. Starting with SQL Server 2017, service packs won't be released since it follows a modern servicing model. The SQL Server team recommends ongoing, proactive installation of cumulative updates as they become available.

Unless specified otherwise, the following versions of SQL Server are supported with all active versions of Configuration Manager. If support for a new SQL Server version is added, the Configuration Manager version that adds that support is noted. Similarly, if support is deprecated, look for details about affected versions of Configuration Manager.

> **IMPORTANT**
> When you use SQL Server Standard for the database at the central administration site, you limit the total number of clients that a hierarchy can support. See Size and scale numbers.

SQL Server 2017: Standard, Enterprise

You can use this version with cumulative update version 2 or higher, as long as your cumulative update version is supported by the SQL lifecycle. This version of SQL can be used for the following sites:

- A central administration site
- A primary site
- A secondary site

SQL Server 2016: Standard, Enterprise

You can use this version with the minimum service pack and cumulative update supported by the SQL lifecycle. This version of SQL can be used for the following sites:

- A central administration site
- A primary site
- A secondary site

SQL Server 2014: Standard, Enterprise

You can use this version with the minimum service pack and cumulative update supported by the SQL lifecycle. This version of SQL can be used for the following sites:

- A central administration site
- A primary site
- A secondary site

SQL Server 2012: Standard, Enterprise

You can use this version with the minimum service pack and cumulative update supported by the SQL lifecycle. This version of SQL can be used for the following sites:

- A central administration site
- A primary site
- A secondary site

SQL Server 2017 Express

You can use this version with cumulative update version 2 or higher, as long as your cumulative update version is supported by the SQL lifecycle. This version of SQL can be used for the following sites:

- A secondary site

SQL Server 2016 Express

You can use this version with the minimum service pack and cumulative update supported by the SQL lifecycle. This version of SQL can be used for the following sites:

- A secondary site

SQL Server 2014 Express

You can use this version with the minimum service pack and cumulative update supported by the SQL lifecycle. This version of SQL can be used for the following sites:

- A secondary site

SQL Server 2012 Express

You can use this version with the minimum service pack and cumulative update supported by the SQL lifecycle. This version of SQL can be used for the following sites:

- A secondary site

Required configurations for SQL Server

The following configurations are required by all installations of SQL Server that you use for a site database, including SQL Server Express. When Configuration Manager installs SQL Server Express as part of a secondary site installation, it automatically creates these configurations.

SQL Server architecture version

Configuration Manager requires a 64-bit version of SQL Server to host the site database.

Database collation

At each site, both the instance of SQL Server that's used for the site and the site database must use the following collation: **SQL_Latin1_General_CP1_CI_AS**.

Configuration Manager supports two exceptions to this collation for the China GB18030 standard. For more information, see International support.

Database compatibility level

Configuration Manager requires that the compatibility level for the site database is no less than the lowest supported SQL Server version for your Configuration Manager version. For instance, beginning with version 1702, you need to have a database compatibility level greater than or equal to 110.

SQL Server features

Only the **Database Engine Services** feature is required for each site server.

Configuration Manager database replication doesn't require the **SQL Server replication** feature. However, this SQL Server configuration is required when you use database replicas for management points.

Windows authentication

Configuration Manager requires **Windows authentication** to validate connections to the database.

SQL Server instance

Use a dedicated instance of SQL Server for each site. The instance can be a **named instance** or the **default instance**.

SQL Server memory

Reserve memory for SQL Server by using SQL Server Management Studio. Set the **Minimum server memory** setting under **Server Memory Options**. For more information about how to configure this setting, see SQL Server memory server configuration options.

- **For a database server that you install on the same computer as the site server**: Limit the memory

for SQL Server to 50 to 80 percent of the available addressable system memory.

- **For a dedicated database server that's remote from the site server**: Limit the memory for SQL Server to 80 to 90 percent of the available addressable system memory.
- **For a memory reserve for the buffer pool of each SQL Server instance in use**:
  - For a central administration site: Set a minimum of 8 GB.
  - For a primary site: Set a minimum of 8 GB.
  - For a secondary site: Set a minimum of 4 GB.

SQL nested triggers

SQL nested triggers must be enabled. For more information, see Configure the nested triggers server configuration option

SQL Server CLR integration

The site database requires SQL Server common language runtime (CLR) to be enabled. This option is enabled automatically when Configuration Manager installs. For more information about CLR, see Introduction to SQL Server CLR Integration.

SQL Server Service Broker (SSB)

The SQL Server Service Broker is required both for intersite replication as well as for a single primary site.

TRUSTWORTHY setting

Configuration Manager automatically enables the SQL TRUSTWORTHY database property. This property is required by Configuration Manager to be **ON**.

Optional configurations for SQL Server

The following configurations are optional for each database that uses a full SQL Server installation.

SQL Server service

You can configure the SQL Server service to run using:

- A *low rights domain user* account:
  - This configuration is a best practice and might require you to manually register the service principal name (SPN) for the account.
- The **local system** account of the computer that runs SQL Server:
  - Use the local system account to simplify the configuration process.
  - When you use the local system account, Configuration Manager automatically registers the SPN for the SQL Server service.
  - Using the local system account for the SQL Server service isn't a SQL Server best practice.

When the computer running SQL Server doesn't use its local system account to run the SQL Server service, configure the SPN of the account that runs the SQL Server service in Active Directory Domain Services. (When the system account is used, the SPN is automatically registered for you.)

For information about SPNs for the site database, see Manage the SPN for the site database server.

For information about how to change the account that is used by the SQL Server service, see SCM Services - Change the service startup account.

SQL Server Reporting Services

SQL Server Reporting Services is required for installing a reporting services point that lets you run reports.

> **IMPORTANT**
> After you upgrade SQL Server from a previous version, you might see the following error: *Report Builder Does Not Exist*. To resolve this error, you must reinstall the reporting services point site system role.

SQL Server ports

For communication to the SQL Server database engine and for intersite replication, you can use the default SQL Server port configurations or specify custom ports:

- **Intersite communications** use the SQL Server Service Broker, which uses port TCP 4022 by default.
- **Intrasite communications** between the SQL Server database engine and various Configuration Manager site system roles use port TCP 1433 by default. The following site system roles communicate directly with the SQL Server database:
  - Management point
  - SMS Provider computer
  - Reporting services point
  - Site server

When a computer running SQL Server hosts a database from more than one site, each database must use a separate instance of SQL Server. Also, each instance must be configured to use a unique set of ports.

> **WARNING**
> Configuration Manager doesn't support dynamic ports. Because SQL Server named instances by default use dynamic ports for connections to the database engine, when you use a named instance, you must manually configure the static port that you want to use for intrasite communication.

If you have a firewall enabled on the computer that is running SQL Server, make sure that it's configured to allow the ports that are being used by your deployment and at any locations on the network between computers that communicate with the SQL Server.

For an example of how to configure SQL Server to use a specific port, see Configure a server to listen on a specific TCP port.

Upgrade options for SQL Server

If you need to upgrade your version of SQL Server, use one of the following methods, from easy to more complex:

- Upgrade SQL Server in-place (recommended)
- Install a new version of SQL Server on a new computer, and then use the database move option of Configuration Manager setup to point your site server to the new SQL Server
- Use backup and recovery. Using backup and recovery for a SQL upgrade scenario is supported. You can ignore the SQL versioning requirement when reviewing Considerations before recovering a site.

Supported Active Directory domains for System Center Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

All System Center Configuration Manager site systems must be members of a supported Windows Server Active Directory domain. Configuration Manager client computers can be domain members or workgroup members.

Requirements and limitations:

- Domain membership applies to site systems that support Internet-based client management in a perimeter network (also known as a DMZ, demilitarized zone, and screened subnet).
- It's not supported to change the following for a computer that hosts a site system role:
  - Domain membership *(This includes removing a site system from the domain, and then rejoining the same domain.)*
  - Domain name
  - Computer name

You must uninstall the site system role (including the site if it's a site server) before making these changes.

Domains with the following domain functional levels are supported:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

Disjoint namespace

Configuration Manager supports installing site systems and clients in a domain that has a disjoint namespace.

A disjoint namespace scenario is one in which the primary Domain Name System (DNS) suffix of a computer doesn't match the Active Directory DNS domain name where that computer resides. The computer that uses the primary DNS suffix that doesn't match is said to be disjoint. Another disjoint namespace scenario occurs if the NetBIOS domain name of a domain controller doesn't match the Active Directory DNS domain name.

The following table identifies the supported scenarios for a disjoint namespace.

SCENARIO	MORE INFORMATION

SCENARIO	MORE INFORMATION
Scenario 1: The primary DNS suffix of the domain controller differs from the Active Directory DNS domain name. Computers that are members of the domain can be either disjoint or not disjoint.	In this scenario, the primary DNS suffix of the domain controller differs from the Active Directory DNS domain name. The domain controller is disjoint in this scenario. Computers that are members of the domain, such as site servers and computers, can have a primary DNS suffix that either matches the primary DNS suffix of the domain controller or matches the Active Directory DNS domain name.
Scenario 2: A member computer in an Active Directory domain is disjoint, even though the domain controller is not disjoint.	In this scenario, the primary DNS suffix of a member computer on which a site system is installed differs from the Active Directory DNS domain name, even though the primary DNS suffix of the domain controller is the same as the Active Directory DNS domain name. In this scenario, you have a domain controller that is not disjoint and a member computer that is disjoint. Member computers that are running the Configuration Manager client can have a primary DNS suffix that either matches the primary DNS suffix of the disjoint site system server or matches the Active Directory DNS domain name.

To allow a computer to access domain controllers that are disjoint, you must change the **msDS-AllowedDNSSuffixes** Active Directory attribute on the domain object container. You must add both DNS suffixes to the attribute.

In addition, to make sure that the DNS suffix search list contains all the DNS namespaces that are deployed within the organization, you must configure the search list for each computer in the domain that is disjoint. Make sure that you include the following in the list of namespaces: the primary DNS suffix of the domain controller, the DNS domain name, and any additional namespaces for other servers that Configuration Manager might interoperate with. You can use the Group Policy Management console to configure the **Domain Name System (DNS) suffix search** list.

> **IMPORTANT**
> When you reference a computer in Configuration Manager, enter the computer by using its Primary DNS suffix. This suffix should match the Fully Qualified Domain Name that is registered as the **dnsHostName** attribute in the Active Directory domain and the Service Principal Name that is associated with the system.

Single label domains

Configuration Manager supports site systems and clients in a single label domain when the following criteria are met:

- The single label domain in Active Directory Domain Services must be configured with a disjoint DNS namespace that has a valid top-level domain.

  For example: The single label domain of Contoso is configured to have a disjoint namespace in DNS of contoso.com. Therefore, when you specify the DNS suffix in Configuration Manager for a computer in the Contoso domain, you specify "Contoso.com" and not "Contoso".

- The Distributed Component Object Model (DCOM) connections between site servers in the system context must be successful by using Kerberos authentication.

Support for Windows features and networks in Configuration Manager

5/9/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article identifies Configuration Manager support for common Windows and networking features.

BranchCache

Use Windows BranchCache with Configuration Manager when you enable it on distribution points, and configure clients to use it in distributed cache mode.

Configure the BranchCache settings on a deployment type for applications, on the deployment for a package, and for task sequences. Starting in version 1802, BranchCache is enabled by default.

When the requirements for BranchCache are met, this feature enables clients in remote locations to obtain content from local clients that have a current cache of the content.

For example, when the first BranchCache-enabled client requests content from a distribution point that's configured as a BranchCache server, the client downloads and caches the content. This content is then made available for clients on the same subnet that requested this content.

These clients also cache the content. Other clients on the same subnet don't have to download content from the distribution point. The content is distributed across multiple clients for future transfers.

Requirements to support BranchCache with Configuration Manager

Configure distribution points

Add the **Windows BranchCache** feature to the site system server that's configured as a distribution point.

- Distribution points on servers that are configured to support BranchCache require no additional configuration.
- You can't add Windows BranchCache to a cloud-based distribution point. Cloud-based distribution points do support the download of content by clients that are configured for Windows BranchCache.

Configure clients

- The clients that can support BranchCache must be configured for BranchCache distributed cache mode.
- The OS setting for BITS client settings must be enabled to support BranchCache.

For information, see configure clients for BranchCache in the Windows documentation.

Configuration Manager supported OS versions with Windows BranchCache

OPERATING SYSTEM	SUPPORT DETAILS
Windows 7 with SP1	Supported by default
Windows 8	Supported by default
Windows 8.1	Supported by default
Windows 10	Supported by default

OPERATING SYSTEM	SUPPORT DETAILS
Windows Server 2008 with SP2	**Requires BITS 4.0**: Install the BITS 4.0 release on Configuration Manager clients by using software updates or software distribution. For more information, see Windows Management Framework. On this OS, the BranchCache client functionality isn't supported for software distribution that's run from the network or for SMB file transfers. Additionally, this OS can't use BranchCache functionality with cloud-based distribution points.
Windows Server 2008 R2	Supported by default
Windows Server 2012	Supported by default
Windows Server 2012 R2	Supported by default
Windows Server 2016	Supported by default

For more information, see BranchCache for Windows in the Windows Server documentation.

Computers in workgroups

Configuration Manager provides support for clients in workgroups.

- Configuration Manager supports moving a client from a workgroup to a domain or from a domain to a workgroup. For more information, see How to install Configuration Manager clients on workgroup computers.

> **NOTE**
> Although clients in workgroups are supported, all site systems must be members of a supported Active Directory domain.

Data deduplication

Configuration Manager supports the use of data deduplication with distribution points on the following operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

> **IMPORTANT**
> The volume that hosts package source files can't be marked for data deduplication. This limitation is because data deduplication uses reparse points. Configuration Manager doesn't support using a content source location with files stored on reparse points.

For more information, see Configuration Manager Distribution Points and Windows Server 2012 Data Deduplication on the Configuration Manager team blog, and Data Deduplication Overview in the Windows Server documentation.

DirectAccess

Configuration Manager supports the DirectAccess feature for communication between clients and site server systems.

- When all the requirements for DirectAccess are met, it enables Configuration Manager clients on the internet to communicate with their assigned site as if they were on the intranet.
- For server-initiated actions, such as remote control and client push installation, the initiating computer must be running IPv6. This protocol must be supported on all intervening networking devices.

Configuration Manager doesn't support the following functionality over DirectAccess:

- OS deployment
- Communication between Configuration Manager sites
- Communication between Configuration Manager site system servers within a site

Dual-boot computers

Configuration Manager can't manage more than one OS on a single computer. If there's more than one OS on a computer to manage, adjust the site's discovery and client installation methods to ensure that the Configuration Manager client is installed only on the OS that has to be managed.

IPv6

In addition to Internet Protocol version 4 (IPv4), Configuration Manager supports Internet Protocol version 6 (IPv6), with the following exceptions:

FUNCTION	EXCEPTION TO IPV6 SUPPORT
Cloud-based distribution points	IPv4 is required to support Microsoft Azure and cloud-based distribution points.
Cloud management gateway	IPv4 is required to support Microsoft Azure and the cloud management gateway.
Mobile devices that are enrolled by Microsoft Intune and the Microsoft service connector	IPv4 is required to support mobile devices that are enrolled by Microsoft Intune and the Microsoft service connector.
Network Discovery	IPv4 is required when you configure a DHCP server to search in Network Discovery.
OS deployment	In version 1802 and prior, IPv4 is required to support OS deployment. Starting in version 1806, enable a PXE responder on a distribution point without Windows Deployment Service. This new PXE responder service supports IPv6. Other aspects of the OS deployment feature, such as capturing or setting static IP addresses during the task sequence, continue to require IPv4.
Wake-up proxy communication	IPv4 is required to support the client wake-up proxy packets.
Windows CE	IPv4 is required to support the Configuration Manager client on Windows CE devices.

Network Address Translation

Network Address Translation (NAT) isn't supported in Configuration Manager, unless the site supports clients that are on the internet and the client detects that it's connected to the internet. For more information about internet-based client management, see Plan for managing internet-based clients.

Specialized storage technology

Configuration Manager works with any hardware that's certified on the Windows Hardware Compatibility List for the version of the OS that the Configuration Manager component is installed on.

Site server roles require NTFS, so that Configuration Manager can set directory and file permissions. Configuration Manager assumes that it has complete ownership of a logical drive. Site systems that run on separate computers can't share a logical partition on any storage technology. However, each computer can use a separate logical partition on the same physical partition of a shared storage device.

Support considerations

- **Storage Area Network**: A Storage Area Network (SAN) is supported when a supported Windows-based server is attached directly to the volume that's hosted by the SAN.
- **Single Instance Storage**: Configuration Manager doesn't support configuration of distribution point package and signature folders on a Single Instance Storage (SIS)-enabled volume.

  Additionally, the cache of a Configuration Manager client isn't supported on a SIS-enabled volume.
- **Removable disk drive**: Configuration Manager doesn't support the installation of Configuration Manager site systems or clients on a removable disk drive.

Support for virtualization environments with Configuration Manager

7/8/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager supports installing the client and site system roles on supported operating systems that run as a virtual machine in the virtualization environments in this article. This support exists even when the virtual machine host (virtualization environment) isn't supported as a client or site server.

For example, you use Microsoft Hyper-V Server 2012 to host a virtual machine that runs Windows Server 2012. You can install the client or site system roles on the virtual machine running Windows Server 2012. You can't install the client on the host running Microsoft Hyper-V Server 2012.

Virtualization environments

- Windows Server 2019
- Windows Server 2016 Note 1
- Microsoft Hyper-V Server 2016 Note 1
- Windows Server 2012 R2
- Microsoft Hyper-V Server 2012
- Windows Server 2012
- Microsoft Hyper-V Server 2008 R2
- Windows Server 2008 R2

Note 1: Nested virtualization

Configuration Manager doesn't support nested virtualization, which is new with Windows Server 2016.

Virtualization environment support

Each virtual computer needs the same or greater hardware and software requirements that you would use for a physical Configuration Manager computer.

To validate that your virtualization environment is supported for Configuration Manager, use the Server Virtualization Validation Program. It includes an online Virtualization Program Support Policy Wizard. For more information, see Windows Server Virtualization Validation Program.

> **NOTE**
> Configuration Manager doesn't support Virtual PC or Virtual Server guest operating systems that run on Mac computers.

Configuration Manager can't manage virtual machines if they're offline. An offline virtual machine image can't be updated nor can inventory be collected by using the Configuration Manager client on the host computer.

No special consideration is given to virtual machines. For example, Configuration Manager might not determine whether an update has to be reapplied to a virtual machine image if the virtual machine has been stopped and restarted without saving the state of the virtual machine to which the update was applied.

Microsoft Azure virtual machines

Configuration Manager can run on virtual machines in Azure just as it runs on-premises within your data center. Use Configuration Manager with Azure virtual machines in the following scenarios:

- **Scenario 1**: Run Configuration Manager on an Azure virtual machine. Use it to manage clients on other Azure virtual machines.
- **Scenario 2**: Run Configuration Manager on an Azure virtual machine. Use it to manage clients that aren't running on Azure.
- **Scenario 3**: Run different Configuration Manager site system roles on Azure virtual machines. Run other roles in your on-premises data center, properly connected to Azure.

The same Configuration Manager requirements for networks, supported configurations, and hardware requirements that apply to installing it on-premises also apply to installation on Azure virtual machines.

For more information, see Configuration Manager on Azure.

> **IMPORTANT**
> Configuration Manager sites and clients that run on Azure virtual machines are subject to the same license requirements as on-premises installations.

Choose a device management solution for Configuration Manager

5/28/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager offers different solutions for managing PCs, servers, and devices. Choose the solution that's right for your organization. Base your decision on the device platforms you need to manage and the management functionality you need.

> **IMPORTANT**
> As of August 14, 2018, hybrid mobile device management is a deprecated feature. For more information, see What is hybrid MDM.

Overview

This article covers the following four device management solutions:

- Configuration Manager client
- On-premises mobile device management (MDM) with Configuration Manager
- Co-management with Microsoft Intune
- Microsoft Exchange

You can use these device management solutions by themselves or in combination with each other. For example, you can use the client-based management approach to manage the computers and servers in your organization, and also use co-management to manage internet-based laptops. By combining approaches this way, you can cover all of your device management needs.

The article also includes two tables that compare the management solutions by the following factors:

- Compare by supported platforms
- Compare by management functionality

Configuration Manager client

This option requires installation of the Configuration Manager client on devices. It provides the most features for managing PCs, servers, and other devices in your environment.

For more information, see Client installation methods.

On-premises MDM

This option uses the device management capabilities built into Windows 10. While not as full-featured as client-based management, on-premises mobile device management provides a lighter touch approach to management. It uses on-premises Configuration Manager resources to manage devices.

For more information, see Manage mobile devices with on-premises infrastructure.

Co-management with Microsoft Intune

Co-management is one of the primary ways to attach your existing Configuration Manager deployment to the Microsoft 365 cloud. It enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune. Co-management lets you cloud-attach your existing investment in Configuration

Manager by adding new functionality.

For more information, see What is co-management?.

Microsoft Exchange

This option uses the Exchange Server connector to connect multiple Exchange servers to Configuration Manager. This centralizes management of devices that can connect to Exchange ActiveSync. You can configure Exchange mobile device management features from the Configuration Manager console. Example features include remote device wipe and the settings control for multiple Exchange servers.

For more information, see Manage mobile devices with Configuration Manager and Exchange.

Compare solutions by supported platforms

PLATFORM	CONFIGURATION MANAGER CLIENT	ON-PREMISES MDM	CONFIGURATION MANAGER WITH EXCHANGE
Android			Yes
iOS			Yes
Mac OS X	Yes		Yes
UNIX/Linux	Yes		Yes
Windows 10	Yes	Yes	Yes
Windows 10 Mobile		Yes	Yes
Windows (previous versions)	Yes		Yes
Windows Server	Yes		Yes
Windows CE	Yes (with mobile device legacy client)		Yes
Windows Embedded	Yes		
Windows Mobile			Yes

For a complete list of supported platforms, see Supported operating systems for clients and devices for System Center Configuration Manager.

Microsoft recommends using Intune to manage Android, iOS, and Windows 10 mobile devices. For more information, see What is Microsoft Intune?

Compare solutions by management functionality

MANAGEMENT FUNCTIONALITY	CONFIGURATION MANAGER CLIENT	ON-PREMISES MDM	CONFIGURATION MANAGER WITH EXCHANGE
Public key infrastructure (PKI) security between the mobile device and Configuration Manager (uses mutual authentication and SSL to encrypt data transfers)	Yes	Yes	
Client installation	Yes		
Support over the internet	Yes		
Discovery	Yes		Yes
Hardware inventory	Yes	Yes	Yes
Software inventory	Yes		Yes
Settings	Yes	Yes	Yes
Software deployment	Yes	Yes	
Monitor with fallback status point	Yes		
Connections to management points	Yes	Yes	
Connections to distribution points	Yes	Yes	
Block from Configuration Manager	Yes	Yes	
Quarantine and block from Exchange Server (and Configuration Manager)			Yes
Remote wipe		Yes	Yes

Design a hierarchy of sites for Configuration Manager

2/12/2019 • 10 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Before installing the first site of a new Configuration Manager hierarchy, it's a good idea to understand:

- The available topologies for Configuration Manager
- The types of available sites and their relationships with each other
- The scope of management that each type of site provides
- The content management options that can reduce the number of sites you need to install

Then plan a topology that efficiently serves your current business needs and can later expand to manage future growth.

When planning, keep in mind limitations for adding additional sites to a hierarchy or a stand-alone site:

- Install a new primary site below a central administration site, up to the supported number of primary sites for the hierarchy.
- Expand a standalone primary site to install a new central administration site, to then install additional primary sites.
- Install new secondary sites below a primary site, up to the supported limit for the primary site and overall hierarchy.
- You can't add a previously installed site to an existing hierarchy to merge two standalone sites. Configuration Manager only supports installation of new sites to an existing hierarchy of sites.

> **NOTE**
> When planning a new installation of Configuration Manager, be aware of the release notes, which detail current issues in the active versions. The release notes apply to all branches of Configuration Manager. When you use the technical preview branch, find issues specific to that branch in the documentation for each version of the technical preview.

Hierarchy topology

Hierarchy topologies range from:

- Simplest: A single standalone primary site
- Most complex: A group of connected primary and secondary sites with a central administration site at the top-level site of the hierarchy

The key driver of the type and count of sites that you use in a hierarchy is usually the number and type of devices you must support.

Standalone primary site

Use a standalone primary site when it can support management of all devices and users. For more information, see Sizing and scale numbers. This topology is also successful when your company's geographic locations can be

served by a single primary site. To help manage network traffic, use multiple management points in boundary groups, and a carefully planned content infrastructure. For more information, see Configure boundary groups and Fundamental concepts for content management.

This topology provides the following benefits:

- Simplified administrative overhead
- Simplified client site assignment and discovery of available resources and services
- Elimination of possible delays introduced by database replication between sites
- Option to expand a standalone primary site into a larger hierarchy with a central administration site. This option enables you to then install new primary sites to expand the scale of your deployment.

Central administration site with one or more child primary sites

Use this topology when you require more than one primary site to support management of all your devices and users. It's required when you need to use more than a single primary site.

This topology provides the following benefits:

- It supports up to 25 primary sites that enable you to extend the scale of your hierarchy.
- You always use the central administration site, unless you reinstall your sites. This option is permanent. You can't detach a child primary site to make it a standalone primary site.

Determine when to use a central administration site

Use a central administration site to configure hierarchy-wide settings and to monitor all sites and objects in the hierarchy. This site type doesn't manage clients directly. It coordinates site-to-site data replication, which includes the configuration of sites and clients throughout the hierarchy.

The following information can help you decide when to install a central administration site:

- The central administration site is the top-level site in a hierarchy.
- When you configure a hierarchy that has more than one primary site, install a central administration site.
  - If you immediately need two or more primary sites, install the central administration site first.
  - When you already have a primary site, and want to then install a central administration site, expand the stand-alone primary site to install the central administration site.
- The central administration site supports only primary sites as child sites.
- The central administration site can't have clients assigned to it.
- The central administration site doesn't support site system roles that directly support clients, such as management points and distribution points.
- Manage all clients in the hierarchy and perform all site management tasks from the Configuration Manager console that is connected to the central administration site. These tasks include installing management points or other site system roles at child primary or secondary sites.
- When you use a central administration site, it's the only place where you see site data from all sites in your hierarchy. This data includes information such as inventory data and status messages.
- Configure discovery operations throughout the hierarchy from the central administration site. From the central administration site, assign discovery methods to run at individual primary sites.
- Manage security throughout the hierarchy by assigning different security roles, security scopes, and

collections to different administrative users. These configurations apply at each site in the hierarchy.

- Configure replication to control communication between sites in the hierarchy. Schedule database replication for site data, and managing the bandwidth for the transfer of file-based data between sites.

Determine when to use a primary site

Use primary sites to manage clients. Install a primary site as a child site below a central administration site, or as the first site of a new hierarchy. A primary site that's the first site of a hierarchy creates a standalone primary site. Both child primary sites and standalone primary sites support secondary sites.

Consider adding additional primary sites for the following reasons:

- To increase the number of devices, manage with a single hierarchy.
- To meet organizational management requirements. For example, you might install a primary site at a remote location to manage the transfer of deployment content across a low-bandwidth network.
    - Consider instead using options to throttle the network bandwidth when transferring data to a distribution point. That content management capability can replace the need to install additional sites.

The following information can help you decide when to install a primary site:

- A primary site can be a standalone primary site or a child primary site in a larger hierarchy. When a primary site is a member of a hierarchy with a central administration site, the sites use database replication to replicate data between the sites. Unless you need to support more clients and devices than a single primary site supports, consider installing a standalone primary site. After you install a standalone primary site, expand it if needed in the future to report to a new central administration site to scale up your deployment.
- A primary site supports only a central administration site as a parent site.
- A primary site supports only secondary sites as child sites, and supports multiple secondary sites.
- Primary sites are responsible for processing all client data from their assigned clients.
- Primary sites use database replication to communicate directly to their central administration site. This behavior is configured automatically when a new site installs.

Determine when to use a secondary site

Use secondary sites to manage the transfer of deployment content and client data across low-bandwidth networks.

You manage a secondary site from a central administration site or the secondary site's direct parent primary site. Secondary sites are attached to a primary site. You can't move them to a different parent site without uninstalling them and then reinstalling them as a child site below the new primary site.

However, you can route content between two peer secondary sites to help manage the file-based replication of deployment content. To transfer client data to a primary site, the secondary site uses file-based replication. A secondary site also uses database replication to communicate with its parent primary site.

Consider installing a secondary site if any of the following conditions apply:

- You don't require a local point of connectivity for an administrative user.
- You're required to manage the transfer of deployment content to sites lower in the hierarchy.
- You're required to manage client information that's sent to sites higher in the hierarchy.

If you don't want to install a secondary site, and you have clients in remote locations, consider the following options:

- Use peer-to-peer technologies such as Windows BranchCache
- Enable distribution points for bandwidth control and scheduling

Use these content management options with or without secondary sites. They help reduce the size of your Configuration Manager infrastructure. For more information about content management options in Configuration Manager, see Determine when to use content management options.

The following information can help you decide when to install a secondary site:

- If a local instance of SQL Server isn't available, secondary site servers automatically install SQL Server Express during site installation.
- Secondary site installation is initiated from the Configuration Manager console, instead of running setup directly on a computer.
- Secondary sites use a subset of the information in the site database. This behavior reduces the amount of data that SQL replicates between the parent primary site and secondary site.
- Secondary sites support the routing of file-based content to other secondary sites that have a common parent primary site.
- Secondary site installations automatically install the management point and distribution point site system roles on the secondary site server.

Determine when to use content management options

If you have clients in remote network locations, consider using one or more content management options instead of a primary or secondary site. The following options often remove the need to install a site:

- Delivery Optimization for Windows 10
- Configuration Manager peer cache
- Windows BranchCache
- Configure distribution points for bandwidth control
- Manually copy content to distribution points (prestage content)

If any of the following conditions apply, consider deploying a distribution point instead of installing another site:

- Your network bandwidth is sufficient for client computers at the remote location to communicate with a management point at the primary site. Clients communicate with a management point to download client policy, send inventory, send reporting status, and send discovery information.
- Background Intelligent Transfer Service (BITS) doesn't provide sufficient bandwidth control for your network requirements.

For more information about content management options in Configuration Manager, see Fundamental concepts for content management.

Beyond hierarchy topology

Along with your initial hierarchy topology, also consider the following questions:

- Which site system roles provide services or capabilities from different sites in the hierarchy?

- How are you managing hierarchy-wide configurations and capabilities in your infrastructure?

The following common considerations are covered in separate articles. This information is important to influence or be influenced by your hierarchy design:

- When you're preparing to Manage computers and devices, consider whether the devices are on-premises, in the cloud, or include user-owned devices (BYOD). Additionally, consider how you'll manage devices that support multiple management options. For example, manage Windows 10 devices with Configuration Manager or though integration with Microsoft Intune. For more information, see Choose a device management solution.
- Understand how your available network infrastructure might affect the flow of data between remote locations. For more information, see Prepare your network environment. Also consider the geographic location of your users and devices, and whether they access your infrastructure through your on-premises network or the internet.
- Plan for a content infrastructure to efficiently distribute the content you deploy to devices you manage. This content may be applications, software updates, or operating systems. For more information, see Manage content and content infrastructure.
- Determine which features and capabilities of Configuration Manager you plan to use. Different features require different site system roles or Windows infrastructure. In a multiple site hierarchy, decide where you deploy them for the most efficient use of your network and server resources.
- Consider security for data and devices, including the use of a public key infrastructure (PKI). For more information, see PKI certificate requirements.

Review the following articles for site-specific configurations:

- Plan for the SMS Provider
- Plan for the site database
- Plan for site system servers and site system roles
- Plan for security
- Managing network bandwidth when deploying content within a site

Consider configurations that span sites and hierarchies

- High availability options for sites and hierarchies
- Extend the Active Directory schema and configure sites to publish site data
- Data transfers between sites
- Fundamentals of role-based administration
- Manage clients on the internet

Plan for the SMS Provider

7/26/2019 • 12 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To manage Configuration Manager, you use a Configuration Manager console that connects to an instance of the **SMS Provider**. By default, an SMS Provider installs on the site server when you install a central administration site or primary site.

About the SMS Provider

The SMS Provider is a Windows Management Instrumentation (WMI) provider that assigns **read** and **write** access to the Configuration Manager database at a site.

- Each central administration site and primary site require at least one SMS Provider. You can install additional providers as needed.
- The **SMS Admins** security group provides access to the SMS Provider. Configuration Manager automatically creates this group on the site server, and on each computer where you install an instance of the SMS Provider. For more information, see SMS Admins.
- Secondary sites don't support the SMS Provider role.

Configuration Manager administrative users use an SMS Provider to access information that's stored in the database. To do so, admins can use the Configuration Manager console, Resource Explorer, tools, and custom scripts. The SMS Provider doesn't interact with Configuration Manager clients. When a Configuration Manager console connects to a site, it queries WMI on the site server to locate an instance of the SMS Provider to use.

The SMS Provider helps enforce Configuration Manager security. It returns only the information that the console user is authorized to view.

Starting in version 1810, the SMS Provider now provides read-only API interoperability access to WMI over HTTPS, called the **administration service**. This REST API can be used in place of a custom web service to access information from the site. For more information, see Administration service.

> **IMPORTANT**
> When each instance of the SMS Provider for a site is offline, Configuration Manager consoles can't connect to the site.

For more information about how to manage the SMS Provider, see Manage the SMS Provider.

Installation prerequisites

To support the SMS Provider, the target server must meet the following prerequisites:

- In the same domain as the site server and the site database site systems
- Can't have a site system role from a different site
- Can't already have an SMS Provider from any site
- Run a supported OS version
- At least 650 MB of free disk space to support the Windows ADK components. For more information about

Windows ADK and the SMS Provider, see OS deployment requirements.

- Enable Windows server role **Web Server (IIS)**

> **NOTE**
> Every SMS Provider attempts to install the administration service, which requires a certificate. This service has a dependency on IIS to bind that certificate to HTTPS port 443. If you enable Enhanced HTTP, then the site binds that certificate using IIS APIs. If your site uses PKI, you need to manually bind a PKI certificate in IIS on the SMS Provider.

Locations

When you install a site, you automatically install the first SMS Provider for the site. You can specify any of the following supported locations for the SMS Provider:

- The site server
- The site database server
- Another server, which meets the installation prerequisites

To view the locations of each SMS Provider for a site:

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and then select the **Sites** node.
2. Select the desired site from the list, and then choose **Properties** in the ribbon.
3. On the **General** tab of the site **Properties**, view the **SMS Provider location** field.

Each SMS Provider supports simultaneous connections from multiple requests. The only limitations on these connections are the number of server connections that are available to Windows, and the available resources on the server to service the connection requests.

After you install a site, you can run Configuration Manager setup on the site server again. Use setup to change the location of an existing SMS Provider, or to install additional SMS Providers at that site. Install only one SMS Provider on a computer. A computer can't host an SMS Provider from more than one site.

Choosing a location

The following sections describe the advantages and disadvantages of installing an SMS Provider on each supported location:

Configuration Manager site server

- **Advantages:**
  - The SMS Provider doesn't use the system resources of the site database computer.
  - This location can provide better performance than an SMS Provider located on a computer other than the site server or site database computer.
- **Disadvantages:**
  - The SMS Provider uses system and network resources that could be dedicated to site server operations.

SQL Server that hosts the site database

- **Advantages:**
  - The SMS Provider doesn't use system resources on the site server.
  - This location can provide the best performance of the three locations, if sufficient server resources

are available.

- **Disadvantages:**
  - The SMS Provider uses system and network resources that could be dedicated to site database operations.
  - When the site database is hosted on a clustered instance of SQL Server, you can't use this location.

Computer other than the site server or site database server

- **Advantages:**
  - SMS Provider doesn't use site server or site database system resources.
  - This type of location lets you deploy additional SMS Providers to provide high availability for connections.
- **Disadvantages:**
  - The SMS Provider performance might be reduced. This behavior is due to the additional network activity that it requires to coordinate with the site server and the site database computer.
  - This server must be always accessible to the site database server, and to all computers with the Configuration Manager console installed.
  - This location can use system resources that would otherwise be dedicated to other services.

Authentication

Starting in version 1810, you can specify the minimum authentication level for administrators to access Configuration Manager sites. This feature enforces administrators to sign in to Windows with the required level. It applies to all components that access the SMS Provider. For example, the Configuration Manager console, SDK methods, and Windows PowerShell cmdlets.

Configure authentication

To configure this setting, first sign in to Windows with the intended authentication level.

> **IMPORTANT**
> This configuration is a hierarchy-wide setting. Before you change this setting, make sure that all Configuration Manager administrators can sign in to Windows with the required authentication level.

To configure this setting, use the following steps:

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. Select **Hierarchy Settings** in the ribbon.
3. Switch to the **Authentication** tab. Select the desired authentication level, and then select **OK**.
   - Only when necessary, select **Add** to exclude specific users or groups. For more information, see Exclusions.

Authentication levels

The following levels are available:

- **Windows authentication**: Require authentication with Active Directory domain credentials. This setting is the previous behavior, and the current default setting. When you update the site, there's no change to the

authentication level.

- **Certificate authentication**: Require authentication with a valid certificate that's issued by a trusted PKI certificate authority. You don't configure this certificate in Configuration Manager. Configuration Manager requires the administrator to be signed into Windows using PKI.
- **Windows Hello for Business authentication**: Require authentication with strong two-factor authentication that's tied to a device and uses biometrics or a PIN. For more information, see Windows Hello for Business.

Exclusions

From the **Authentication** tab of Hierarchy Settings, you can also exclude certain users or groups. Use this option sparingly. For example, when specific users require access to the Configuration Manager console, but can't authenticate to Windows at the required level. It may also be necessary for automation or services that run under the context of a system account.

About SMS Provider languages

The SMS Provider operates independently of the display language of the server where you install it.

When an administrative user or Configuration Manager process requests data by using the SMS Provider, it attempts to return that data in a format that matches the OS language of the requesting computer.

The way it attempts to match the language is indirect. The SMS Provider doesn't translate information from one language to another. When it returns data for display in the Configuration Manager console, the display language of the data depends on the source of the object and type of storage.

When Configuration Manager stores data for an object in the database, the available languages depend on the following factors:

- Configuration Manager stores objects that it creates by using support for multiple languages. It stores the object in the site database by using the languages that you configure for the site when you run setup. The Configuration Manager console displays these objects in the display language of the requesting computer, when that language is available for the object. If the console can't display the object in the display language of the requesting computer, it displays the object in the default language, which is English.
- Configuration Manager stores objects that an administrative user creates by using the language that was used to create the object. These objects display in the Configuration Manager console in this same language. The SMS Provider can't translate them, and they don't have multiple language options.

Use multiple SMS Providers

After a site completes installation, you can install additional SMS Providers for the site. To install additional SMS Providers, run Configuration Manager setup on the site server.

Consider installing additional SMS Providers when any of the following are true:

- Many administrative users need to use the Configuration Manager console and connect to a site at the same time.
- You use the Configuration Manager SDK, or other products, that might introduce frequent calls to the SMS Provider.
- You have a business requirement for high availability of the SMS Provider.

When you install multiple SMS Providers at a site, and a connection request is made, the site randomly assigns each new connection request to use an installed SMS Provider. You can't specify the SMS Provider to use with a specific connection session.

> **NOTE**
> Consider the advantages and disadvantages of each SMS Provider location. For more information, see Locations. Balance these considerations with the information that you can't control which SMS Provider is used for each new connection.

When you first connect a Configuration Manager console to a site, the connection queries WMI on the site server. This query identifies an instance of the SMS Provider that the console uses. This specific instance of the SMS Provider remains in use by the console until the session ends. If the session ends because the SMS Provider server is unavailable on the network, when you reconnect the console to the site, it repeats the initial query. It's possible the site assigns the same SMS Provider instance that's not available. If this behavior occurs, attempt to reconnect the console until the site returns an available SMS Provider.

About the SMS Provider namespace

The Configuration Manager WMI schema defines the structure of the SMS Provider. Schema namespaces describe the location of Configuration Manager data within the SMS Provider schema. The following table contains some of the common namespaces that the SMS Provider uses:

NAMESPACE	DESCRIPTION
`Root\SMS\site_<site code>`	The SMS Provider, which is extensively used by the Configuration Manager console, Resource Explorer, Configuration Manager tools, and scripts.
`Root\SMS\SMS_ProviderLocation`	The location of the SMS Provider computers for a site.
`Root\CIMv2`	The location inventoried for WMI namespace information during hardware and software inventory.
`Root\CCM`	Configuration Manager client configuration policies and client data.
`Root\CIMv2\SMS`	The location of inventory reporting classes that the inventory client agent collects. Clients compile these settings during computer policy evaluation. These settings are based on the client settings configuration for the computer.

OS deployment requirements

The computer where you install an instance of the SMS Provider requires a supported version of the Windows ADK.

For more information about this requirement, see Infrastructure requirements for OS deployment and Support for Windows 10.

When you manage OS deployments, the Windows ADK allows the SMS Provider to complete various tasks, such as:

- View WIM file details
- Add driver files to existing boot images
- Create boot ISO files

The Windows ADK installation can require up to 650 MB of free disk space on each computer that installs the SMS Provider. This high disk space requirement is necessary for Configuration Manager to install the Windows PE boot

images.

Administration service

> **TIP**
> This feature was first introduced in version 1810 as a pre-release feature. Beginning with version 1906, it's no longer a pre-release feature.

Starting in version 1810, the SMS Provider provides read-only API interoperability access to WMI over HTTPS, called the **administration service**. This REST API can be used in place of a custom web service to access information from the site.

The **administration service** URL format is `https://<servername>/AdminService/wmi/<ClassName>` where `<servername>` is the server where the SMS Provider is installed and `<ClassName>` is a valid Configuration Manager WMI class name. In version 1810, this class name doesn't include the `SMS_` prefix. In version 1902 and later, this class name is the same as the WMI class name.

For example:

- 1810: `https://servername/AdminService/wmi/Site`
- 1902 and later: `https://servername/AdminService/wmi/SMS_Site`

> **NOTE**
> The administration service class names are case-sensitive. Make sure to use the proper capitalization, for example SMS_Site.

Make direct calls to this service with the Windows PowerShell cmdlet Invoke-RestMethod.

> **TIP**
> You can use this cmdlet in a task sequence. This action lets you access information from the site without requiring a custom web service to interface with the WMI provider.

You can also use it to access site data from Power BI using the OData connector option.

The administration service logs its activity to the **adminservice.log** file.

Enable the administration service through the CMG

The **SMS Provider** appears as a role with an option to allow communication over the cloud management gateway (CMG). The current use for this setting is to enable application approvals via email from a remote device. For more information, see Approve applications.

Prerequisites

- The server that hosts the SMS Provider requires .NET 4.5.2 or later.
  - Starting in version 1902, this prerequisite is version .NET 4.5 or later.
- Enable the SMS Provider to use a certificate. Use one of the following options:
  - Enable Enhanced HTTP (recommended)

> **NOTE**
> When the site creates a certificate for the SMS Provider, it won't be trusted by the web browser on the client. Based on your security settings, accessing the REST provider, you may see a security warning.

- Manually bind a PKI-based certificate to port 443 in IIS on the server that hosts the SMS Provider role

Process to enable the API through the CMG

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Servers and Site System Roles** node.
2. Select the server with the **SMS Provider** role.
3. In the details pane, select the **SMS Provider** role, and select **Properties** in the ribbon on the **Site Role** tab.
4. Select the option to **Allow Configuration Manager cloud management gateway traffic for administration service**.

Enable the Configuration Manager console to use the administration service

Starting in version 1906, enable some nodes of the Configuration Manager console to use the administration service. This change allows the console to communicate with the SMS Provider over HTTPS instead of via WMI.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. In the ribbon, select **Hierarchy Settings**.
2. On the **General** page, select the option to **Enable the Configuration Manager console to use the administration service**.

In version 1906, it only affects the following nodes under the **Security** node in the **Administration** workspace:

- Administrative Users
- Security Roles
- Security Scopes
- Console Connections

When you select one of these nodes, if the following error message displays:

Configuration Manager can't connect to the administration service

Review the information below the error. Then verify that the administration service is enabled, configured, and functional.

Plan for the site database for System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The site database server is a computer that runs a supported version of Microsoft SQL Server. SQL Server is used to store information for Configuration Manager sites. Each site in a Configuration Manager hierarchy contains a site database and a server that is assigned the site database server role.

- For central administration sites and primary sites, you can install SQL Server on the site server, or you can install SQL Server on a computer other than the site server.
- For secondary sites, you can use SQL Server Express instead of a full SQL Server installation. The database server must, however, be run on the secondary site server.
- For SQL Availability Group usage the Database Recovery Model must be set to FULL
- For non-SQL Availability Group usage the Database Recovery Model must be set to SIMPLE

Further information on SQL Recovery Modes can be found in Recovery Models (SQL Server).

The following SQL Server configurations can be used to host the site database:

- The default instance of SQL Server
- A named instance on a single computer running SQL Server
- A named instance on a clustered instance of SQL Server
- A SQL Server AlwaysOn availability group (beginning with version 1602 of System Center Configuration Manager)

To host the site database, the SQL Server must meet the requirements detailed in Support for SQL Server versions for System Center Configuration Manager.

Remote database server location considerations

If you use a remote database server computer, ensure that the intervening network connection is a high-availability, high-bandwidth network connection. The site server and some site system roles must constantly communicate with the remote server that is hosting the site database.

- The amount of bandwidth required for communications to the database server depends on a combination of many different site and client configurations. Therefore, the actual bandwidth required cannot be adequately predicted.
- Each computer that runs the SMS Provider and that connects to the site database increases network bandwidth requirements.
- The computer that runs SQL Server must be located in a domain that has two-way trust with the site server and all computers running the SMS Provider.
- You cannot use a clustered SQL Server for the site database server when the site database is co-located with the site server.

Typically, a site system server supports site system roles from only a single Configuration Manager site. You can, however, use different instances of SQL Server, on clustered or non-clustered servers running SQL Server, to host a database from different Configuration Manager sites. To support databases from different sites, you must configure each instance of SQL Server to use unique ports for communication.

Plan for site system servers and site system roles in Configuration Manager

7/26/2019 • 10 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Each Configuration Manager site you install includes a site server that's a **site system server**. The site can also include additional site system servers on computers that are remote from the site server. Site system servers (the site server or a remote site system server) support **site system roles**.

Site system servers

When you install a site system role on a computer, that computer becomes a site system server. At each site, you can install one or more additional site system servers. You don't have to install additional site system servers, and can choose to run all site system roles directly on the site server computer. Each site system server supports one or more site system roles. Additional servers can help expand the capabilities and capacity of a site by sharing the processing load that site system roles place on a server.

When considering the addition of a site system server, ensure the server meets prerequisites for the intended use. Also add it on a network location that has sufficient bandwidth to communicate with expected endpoints. These endpoints include the site server, domain resources, a cloud-based location, site system servers, and clients.

Site system roles

Install site system roles on a server to provide additional capabilities to the site. Examples include:

- Additional management points so that the site can support more devices, up to the site's supported capacity.
- Additional distribution points to expand your content infrastructure, improving the performance of content distributions to devices.
- One or more feature-specific site system roles. For example, a software update point lets you manage software updates for managed devices. A reporting services point lets you run reports to monitor, understand, and share information about your environment.

Different Configuration Manager sites can support different sets of site system roles. The supported set of site system roles depends on the type of site. (The types of sites include a central administration site, primary sites, or secondary sites.) The topology of your hierarchy can limit the placement of some roles at certain site types. For example, the service connection point is only supported at the top-tier site of the hierarchy. The top-tier site might be a central administration site or a standalone primary site. This role isn't supported at a child primary site or at secondary sites.

After a site installs, you can move the location of some site system roles from their default location on the site server to another server. For example, the management point or distribution point roles install by default on a primary or secondary site server. Also install additional instances of some site system roles to expand the capabilities of your site, and to meet your business requirements. Some roles are required, while others are optional.

Configuration Manager site server

This role identifies the server where Configuration Manager setup is run to install a site, or the server on which you install a secondary site. You can't move or uninstall this role until the site is uninstalled.

Configuration Manager site system

This role is assigned to any computer on which you either install a site or install a site system role. You can't move or uninstall this role until you remove the last site system role from the computer.

Configuration Manager component site system role

This role identifies a site system that runs an instance of the **SMS Executive** service. It's required to support other roles, like management points. You can't move or uninstall this role until you remove the last applicable site system role from the computer.

Configuration Manager site database server

The site assigns this role to site system servers that hold an instance of the site database. Only move this role to a new server by running setup to modify the site to use a different instance of SQL Server to host the site database.

SMS Provider

The site assigns this role to each computer that hosts an instance of the SMS Provider. The provider is the interface between a Configuration Manager console and the site database. By default, this role automatically installs on the site server of a central administration site and primary sites. Install additional instances at each site to provide access to additional administrative users or for redundancy.

To install additional providers, run Configuration Manager setup to Manage the SMS Provider. Then install additional providers on additional computers. Only install one instance of the SMS Provider on a computer. That computer must be in the same domain as the site server.

Application catalog web service point

> **IMPORTANT**
>
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features

A site system role that provides software information to the application catalog website from the software library. Although this role is supported only at primary sites, you can install multiple instances of this role at a site, or at multiple sites in the same hierarchy.

Application catalog website point

> **IMPORTANT**
>
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features

A site system role that provides users with a list of available software from the application catalog. Although this role is supported only at primary sites, you can install multiple instances of this role at a site, or at multiple sites in

the same hierarchy.

Asset Intelligence synchronization point

A site system role that connects to Microsoft to download information for the Asset Intelligence catalog. This role also uploads uncategorized titles, so that Microsoft can consider them for future inclusion in the catalog. A hierarchy supports only a single instance of this role at the top-tier site of your hierarchy. If you expand a standalone primary site into a larger hierarchy, uninstall this role from the primary site. Then install it at the central administration site.

For more information, see Asset Intelligence in Configuration Manager.

Certificate registration point

A site system role that communicates with a server that runs the Network Device Enrollment Service (NDES). This role manages device certificate requests that use the Simple Certificate Enrollment Protocol (SCEP). This role is supported only at primary sites and the central administration site.

Although a single certificate registration point can provide functionality to an entire hierarchy, you may want to install multiple instances of this role at a site, and at multiple sites in the same hierarchy. This design helps with load balancing. When multiple instances exist in a hierarchy, clients are randomly assigned to one of the certificate registration points.

Each certificate registration point requires access to a separate NDES instance. You can't configure two or more certificate registration points to use the same NDES instance. Additionally, don't install the certificate registration point on the same server that runs NDES.

Cloud management gateway connection point

A site system role for communicating with the cloud management gateway.

Data warehouse service point

Use the data warehouse service point to store and report on long-term historical data in your Configuration Manager environment. For more information, see Data warehouse.

Distribution point

A site system role that contains source files for clients to download, for example:

- Application content
- Software packages
- Software updates
- OS images
- Boot images

By default, this role installs on the site server when you install a new primary or secondary site. This role isn't supported at a central administration site. Install multiple instances of this role at a supported site, and at multiple sites in the same hierarchy. For more information, see Fundamental concepts for content management, and Manage content and content infrastructure.

Endpoint Protection point

A site system role that Configuration Manager uses to accept the Endpoint Protection license terms, and to configure the default membership for Cloud Protection Service. A hierarchy only supports a single instance of this role, and that must be at the top-tier site. If you expand a standalone primary site into a larger hierarchy, uninstall this role from the primary site, and then install it at the central administration site. For more information, see Endpoint Protection in Configuration Manager.

Enrollment point

A site system role that uses PKI certificates for Configuration Manager to enroll mobile devices and macOS

computers. Although this role is supported only at primary sites, you can install multiple instances of this role at a site, or at multiple sites in the same hierarchy.

If a user enrolls mobile devices by using Configuration Manager, and the user's Active Directory account is in a forest that's untrusted by the site server's forest, install an enrollment point in the user's forest. Then Configuration Manager can authenticate the user.

Enrollment proxy point

A site system role that manages Configuration Manager enrollment requests from mobile devices and macOS computers. Although this role is supported only at primary sites, you can install multiple instances of this role at a site, or at multiple sites in the same hierarchy.

When you support mobile devices on the internet, install an enrollment proxy point in a perimeter network, and install one on the intranet.

Exchange Server connector

For information about this role, see Manage mobile devices with Configuration Manager and Exchange.

Fallback status point

A site system role that helps you monitor client installation. It identifies clients that are unmanaged because they can't communicate with their management point. Although this role is supported only at primary sites, you can install multiple instances of this role at a site, and at multiple sites in the same hierarchy.

Management point

A site system role that provides policy and service location information to clients. It also receives configuration data from clients.

By default, this role installs on the site server when you install a new primary or secondary site. Primary sites support multiple instances of this role. Secondary sites support a single management point. Also referred to as a proxy management point, this role at a secondary site provides a local point of contact for clients to obtain computer and user policies.

Set up management points to support either HTTP or HTTPs. They can also support mobile devices that you manage with Configuration Manager on-premises mobile device management (MDM). To help reduce the processing load placed on the site database server by management points as they service requests from clients, use Database replicas for management points.

Reporting services point

A site system role that integrates with SQL Server Reporting Services to create and manage reports for Configuration Manager. This role is supported at primary sites and the central administration site, and you can install multiple instances of this role at a supported site. For more information, see Planning for reporting.

Service connection point

A site system role that uploads usage data from your site, and is required to make updates for Configuration Manager available in the console. This role also helps to manage mobile devices with Microsoft Intune and on-premises MDM. A hierarchy only supports a single instance of this role, and that must be at the top-tier site of your hierarchy. If you expand a standalone primary site into a larger hierarchy, uninstall this role from the primary site, and then install it at the central administration site. For more information, see About the service connection point.

Software update point

A site system role that integrates with Windows Server Update Services (WSUS) to provide software updates to Configuration Manager clients. This role is supported at all sites:

- Install this site system at the central administration site to synchronize with WSUS.

- Set up each instance of this role at child primary sites to synchronize with the central administration site.
- When data transfer across the network is slow, consider installing a software update point in secondary sites.

For more information, see Plan for software updates.

State migration point

When you migrate a computer to a new operating system, this site system role stores user state data. This role is supported at primary sites and at secondary sites. Install multiple instances of this role at a site, and at multiple sites in the same hierarchy. For more information about storing user state when you deploy an OS, see Manage user state.

Next steps

Some Configuration Manager site system roles require connections to the internet. If your environment requires internet traffic to use a proxy server, configure these site system roles to use the proxy. For more information, see Proxy server support.

Fundamental concepts for content management in Configuration Manager

8/26/2019 • 15 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager supports a robust system of tools and options to manage software content. Software deployments such as applications, packages, software updates, and OS deployments all need content. Configuration Manager stores the content on both site servers and distribution points. This content requires a large amount of network bandwidth when it's being transferred between locations. To plan and use the content management infrastructure effectively, first understand the available options and configurations. Then consider how to use them to best fit your networking environment and content deployment needs.

> **TIP**
> For more information about the content distribution process and to find help in diagnosing and resolving general content distribution problems, see Understanding and Troubleshooting Content Distribution in Microsoft Configuration Manager.

The following sections are key concepts for content management. When a concept requires additional or complex information, links are provided to direct you to those details.

Accounts used for content management

The following accounts can be used with content management:

Network access account

Used by clients to connect to a distribution point and access content. By default, the computer account is tried first.

This account is also used by pull-distribution points to download content from a source distribution point in a remote forest.

Starting in version 1806, some scenarios no longer require a network access account. You can enable the site to use Enhanced HTTP with Azure Active Directory authentication.

For more information, see Network access account.

Package access account

By default, Configuration Manager grants access to content on a distribution point to the generic access accounts Users and Administrators. However, you can configure additional permissions to restrict access.

For more information, see Package access account.

Bandwidth throttling and scheduling

Both throttling and scheduling are options that help you control when content is distributed from a site server to distribution points. These capabilities are similar to, but not directly related to bandwidth controls for site-to-site file-based replication.

For more information, see Manage network bandwidth.

Binary differential replication

Configuration Manager uses binary differential replication (BDR) to update content that you previously distributed to other sites or to remote distribution points. To support BDR's reduction of bandwidth usage, install the **Remote Differential Compression** feature on distribution points. For more information, see Distribution point prerequisites.

BDR minimizes the network bandwidth used to send updates for distributed content. It resends only the new or changed content instead of sending the entire set of content source files each time you change those files.

When BDR is used, Configuration Manager identifies the changes that occur to source files for each set of content that you previously distributed.

- When files in the source content change, the site creates a new incremental version of the content. It then replicates only the changed files to destination sites and distribution points. A file is considered changed if you renamed or moved it, or if you changed the contents of the file. For example, if you replace a single driver file for a driver package that you previously distributed to several sites, only the changed driver file is replicated.
- Configuration Manager supports up to five incremental versions of a content set before it resends the entire content set. After the fifth update, the next change to the content set causes the site to create a new version of the content set. Configuration Manager then distributes the new version of the content set to replace the previous set and any of its incremental versions. After the new content set is distributed, later incremental changes to the source files are again replicated by BDR.

BDR is supported between each parent and child site in a hierarchy. BDR is supported within a site between the site server and its regular distribution points. However, pull-distribution points and cloud distribution points don't support BDR to transfer content. Pull-distribution points support file-level deltas, transferring new files, but not blocks within a file.

Applications always use binary differential replication. BDR is optional for packages and isn't enabled by default. To use BDR for packages, enable this functionality for each package. Select the option **Enable binary differential replication** when you create or edit a package.

BDR or delta replication

The following lists summarize the differences between *binary differential replication* (BDR) and *delta replication*.

Summary of binary differential replication

- Configuration Manager's term for Windows **Remote Differential Compression**
- *Block*-level differences
- Always enabled for apps
- Optional on legacy packages
- If a file already exists on the distribution point, and there's a change, the site uses BDR to replicate the block-level change instead of the entire file.

Summary of delta replication

- *File*-level differences
- On by default, not configurable
- When a package changes, the site checks for changes to the individual files instead of the entire package.
  - If a file changes, use BDR to do the work
  - If there's a new file, copy the new file

Peer caching technologies

Configuration Manager supports several options for managing content between peer devices on the same network:

- BranchCache
- Delivery Optimization
- Configuration Manager peer cache

Use the following table to compare major features of these technologies:

FEATURE	PEER CACHE	DELIVERY OPTIMIZATION	BRANCHCACHE
Across subnets	Yes	Yes	No
Throttle bandwidth	Yes (BITS)	Yes (native)	Yes (BITS)
Partial content	Yes	Yes	Yes
Control cache size on disk	Yes	Yes	Yes
Peer source discovery	Manual (client setting)	Automatic	Automatic
Peer discovery	Via management point using boundary groups	DO cloud service	Broadcast
Reporting	Client data sources dashboard	Client data sources dashboard	Client data sources dashboard
WAN usage control	Boundary groups	DO GroupID	Subnet only
Supported content	All ConfigMgr content	Windows updates, drivers, store apps	All ConfigMgr content
Policy control	Client agent settings	Client agent settings (partial)	Client agent settings

Recommendations

- Modern management: If you're already using modern tools such as Intune, implement Delivery Optimization
- Configuration Manager and co-management: Use a combination of peer cache and Delivery Optimization. Use peer cache with on-premises distribution points, and use Delivery Optimization for cloud scenarios.
- Existing BranchCache implemented: Use all three technologies in parallel. Use peer cache and Delivery Optimization for scenarios that aren't supported by BranchCache.

BranchCache

BranchCache is a Windows technology. Clients that support BranchCache, and have downloaded a deployment that you configure for BranchCache, then serve as a content source to other BranchCache-enabled clients.

For example, you have a distribution point that runs Windows Server 2012 or later, and is configured as a BranchCache server. When the first BranchCache-enabled client requests content from this server, the client downloads that content and caches it.

- That client then makes the content available for additional BranchCache-enabled clients on the same subnet that also cache the content.
- Other clients on the same subnet don't have to download content from the distribution point.
- The content is distributed across multiple clients for future transfers.

For more information, see Support for Windows BranchCache.

Delivery Optimization

You use Configuration Manager boundary groups to define and regulate content distribution across your corporate network and to remote offices. Windows Delivery Optimization is a cloud-based, peer-to-peer technology to share content between Windows 10 devices. Configure Delivery Optimization to use your boundary groups when sharing content among peers. Client settings apply the boundary group identifier as the Delivery Optimization group identifier on the client. When the client communicates with the Delivery Optimization cloud service, it uses this identifier to locate peers with the content. For more information, see delivery optimization client settings.

Delivery Optimization is the recommended technology to optimize Windows 10 update delivery of express installation files for Windows 10 quality updates.

Delivery Optimization In-Network Cache

Starting in version 1906, you can install a Delivery Optimization In-Network Cache (DOINC) server on your distribution points. By caching this content on-premises, your clients can benefit from the Delivery Optimization feature, but you can help to protect WAN links.

This cache server acts as an on-demand transparent cache for content downloaded by Delivery Optimization. Use client settings to make sure this server is offered only to the members of the local Configuration Manager boundary group.

This cache is separate from Configuration Manager's distribution point content. If you choose the same drive as the distribution point role, it stores content separately.

For more information, see Delivery Optimization In-Network Cache in Configuration Manager.

Peer cache

Client peer cache helps you manage deployment of content to clients in remote locations. Peer cache is a built-in Configuration Manager solution that enables clients to share content with other clients directly from their local cache.

First deploy client settings that enable peer cache to a collection. Then members of that collection can act as a peer content source for other clients in the same boundary group.

Starting in version 1806, client peer cache sources can divide content into parts. These parts minimize the network transfer to reduce WAN utilization. The management point provides more detailed tracking of the content parts. It tries to eliminate more than one download of the same content per boundary group.

For more information, see Peer cache for Configuration Manager clients.

Windows PE peer cache

When you deploy a new OS with Configuration Manager, computers that run the task sequence can use Windows PE peer cache. They download content from a peer cache source instead of from a distribution point. This behavior helps minimize WAN traffic in branch office scenarios where there's no local distribution point.

For more information, see Windows PE peer cache.

Windows LEDBAT

Windows Low Extra Delay Background Transport (LEDBAT) is a network congestion control feature of Windows

Server to help manage background network transfers. For distribution points running on supported versions of Windows Server, enable an option to help adjust network traffic. Then clients only use network bandwidth when it's available.

For more information on Windows LEDBAT in general, see the New transport advancements blog post.

For more information on how to use Windows LEDBAT with Configuration Manager distribution points, see the setting to **Adjust the download speed to use the unused network bandwidth (Windows LEDBAT)** when you Configure the general settings of a distribution point.

Client locations

The following are locations that clients access content from:

- **Intranet** (on-premises):
  - Distribution points can use HTTP or HTTPs.
  - Only use a cloud distribution point for fallback when on-premises distribution points aren't available.
- **Internet**:
  - Requires internet-facing distribution points to accept HTTPS.
  - Can use a cloud distribution point or cloud management gateway (CMG).

    Starting in version 1806, a CMG can also serve content to clients. This functionality reduces the required certificates and cost of Azure VMs. For more information, see Modify a CMG.
- **Workgroup**:
  - Requires distribution points to accept HTTPS.
  - Can use a cloud distribution point or CMG.

Content source priority

When a client needs content, it makes a content location request to the management point. The management point returns a list of source locations that are valid for the requested content. This list varies depending upon the specific scenario, technologies in use, site design, boundary groups, and deployment settings. The following list contains all of the possible content source locations that a client can use, in the order in which it prioritizes them:

1. The distribution point on the same computer as the client
2. A peer source in the same network subnet
3. A distribution point in the same network subnet
4. A peer source in the same boundary group
5. A distribution point in the current boundary group
6. A distribution point in a neighbor boundary group configured for fallback
7. A distribution point in the default site boundary group
8. The Windows Update cloud service
9. An internet-facing distribution point
10. A cloud distribution point in Azure

> **NOTE**
> Delivery Optimization isn't applicable to this source prioritization. This list is how the Configuration Manager client finds content. The Windows Update Agent downloads content for Delivery Optimization. If the Windows Update Agent can't find the content, then the Configuration Manager client uses this list to search for it.

Content library

The content library is the single-instance store of content in Configuration Manager. This library reduces the overall size of content that you distribute.

- Learn more about the content library.
- Use the content library cleanup tool to remove content that is no longer associated with an application.

Distribution points

Configuration Manager uses distribution points to store files that are required for software to run on client computers. Clients must have access to at least one distribution point from which they can download the files for content that you deploy.

The basic (non-specialized) distribution point is commonly referred to as a standard distribution point. There are two variations on the standard distribution point that receive special attention:

- **Pull-distribution point**: A variation of a distribution point where the distribution point obtains content from another distribution point (a source distribution point). This process is similar to how clients download content from distribution points. Pull-distribution points can help you avoid network bandwidth bottlenecks that occur when the site server must directly distribute content to each distribution point. Use a pull-distribution point.
- **Cloud distribution point**: A variation of a distribution point that's installed on Microsoft Azure. Learn how to use a cloud distribution point.

Standard distribution points support a range of configurations and features:

- Use controls such as **schedules** or **bandwidth throttling** to help control this transfer.
- Use other options, including **prestaged content**, and **pull-distribution points** to minimize and control network consumption.
- **BranchCache**, **peer cache**, and **Delivery Optimization** are peer-to-peer technologies to reduce the network bandwidth that's used when you deploy content.
- There are different configurations for OS deployments, such as **PXE** and **Multicast**
- Options for **mobile devices**

Cloud and pull distribution points support many of these same configurations, but have limitations that are specific to each distribution point variation.

Distribution point groups

Distribution point groups are logical groupings of distribution points that can simplify content distribution.

For more information, see Manage distribution point groups.

Distribution point priority

The distribution point priority value is based on how long it took to transfer previous deployments to that distribution point.

- This value is self-tuning. It's set on each distribution point to help Configuration Manager more quickly transfer content to more distribution points.
- When you distribute content to multiple distributions points at the same time, or to a distribution point group, the site first sends the content to the server with the highest priority. Then it sends that same content to a distribution point with a lower priority.
- Distribution point priority doesn't replace the distribution priority for packages. Package priority remains the deciding factor of when the site sends different content.

For example, you have a package that has a high package priority. You distribute it to a server with a low distribution point priority. This high priority package always transfers before a package that has a lower priority. The package priority applies even if the site distributes lower priority packages to servers with higher distribution point priorities.

The high priority of the package ensures that Configuration Manager distributes that content to distribution points before it sends any packages with a lower priority.

> **NOTE**
>
> Pull-distribution points also use a concept of priority to order the sequence of their source distribution points.
>
> - The distribution point priority for content transfers to the server is distinct from the priority that pull-distribution points use. Pull-distribution points use their priority when they search for content from a source distribution point.
> - For more information, see Use a pull-distribution point.

Fallback

Several things have changed with Configuration Manager current branch in the way that clients find a distribution point that has content, including fallback.

Clients that can't find content from a distribution point that's associated with their current boundary group fall back to use content source locations associated with neighbor boundary groups. To be used for fallback, a neighbor boundary group must have a defined relationship with the client's current boundary group. This relationship includes a configured time that must pass before a client that can't find content locally includes content sources from the neighbor boundary group as part of its search.

The concepts of preferred distribution points are no longer used, and settings for **Allow fallback source locations for content** are no longer available or enforced.

For more information, see Boundary groups.

Network bandwidth

To help manage the amount of network bandwidth that's used when you distribute content, you can use the following options:

- **Prestaged content**: Transferring content to a distribution point without distributing the content across the network.
- **Scheduling and throttling**: Configurations that help you control when and how content is distributed to distribution points.

For more information, see Manage network bandwidth.

Network connection speed to content source

Several things have changed with Configuration Manager current branch in the way that clients find a distribution point that has content. These changes include the network speed to a content source.

Network connection speeds that define a distribution point as **Fast** or **Slow** are no longer used. Instead, each site system that's associated with a boundary group is treated the same.

For more information, see Boundary groups.

On-demand content distribution

On-demand content distribution is an option for individual application and package deployments. This option enables on-demand content distribution to preferred servers.

- To enable this setting for a deployment, enable: **Distribute the content for this package to preferred distribution points**.
- When you enable this option for a deployment, and a client requests that content but the content isn't available on any of the client's preferred distribution points, Configuration Manager automatically distributes that content to the client's preferred distribution points.
- Although this triggers Configuration Manager to automatically distribute the content to that client's preferred distribution points, the client might obtain that content from other distribution points before the preferred distribution points for the client receive the deployment. When this behavior occurs, the content will then be present on that distribution point for use by the next client that seeks that deployment.

For more information, see Boundary groups.

Package transfer manager

Package transfer manager is the site server component that transfers content to distribution points on other computers.

For more information, see Package transfer manager.

Prestage content

Prestaging content is a process of transferring content to a distribution point without distributing the content across the network.

For more information, see Manage network bandwidth.

Use a cloud distribution point in Configuration Manager

8/6/2019 • 17 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

> **IMPORTANT**
>
> The implementation for sharing content from Azure has changed. Use a content-enabled cloud management gateway by enabling the option to **Allow CMG to function as a cloud distribution point and serve content from Azure storage**. For more information, see Modify a CMG.
>
> You won't be able to create a traditional cloud distribution point in the future. For more information, see Removed and deprecated features.

A cloud distribution point is a Configuration Manager distribution point that is hosted as Platform-as-a-Service (PaaS) in Microsoft Azure. This service supports the following scenarios:

- Provide software content to internet-based clients without additional on-premises infrastructure
- Cloud-enable your content distribution system
- Reduce the need for traditional distribution points

This article helps you learn about the cloud distribution point, plan for its use, and design your implementation. It includes the following sections:

Features and benefits

Features

The cloud distribution point supports several features that are also offered by on-premises distribution points:

- Manage cloud distribution points individually or as members of distribution point groups
- Use a cloud distribution point as a fallback content location
- Supports both intranet and internet-based clients

Benefits

The cloud distribution point provides the following additional benefits:

- The site encrypts the content before sending it to the cloud distribution point in Azure.
- To meet changing demands for content requests by clients, manually scale the cloud service in Azure. This action doesn't require that you install and provision additional distribution points in Configuration Manager.
- Supports content download from clients configured for other content technologies, such as Windows BranchCache and alternate content providers.
- Starting in version 1806, use cloud distribution points as source locations for pull-distribution points.

Topology design

Deployment and operation of the cloud distribution point includes the following components:

- A **cloud service** in Azure. The site distributes content to this service, which stores it in Azure cloud storage. The management point provides to clients this content location in the list of available sources as appropriate.
- A **management point** site system role services client requests per normal.
  - On-premises clients typically use an on-premises management point.
  - Internet-based clients either use a cloud management gateway, or an internet-based management point.
- The cloud distribution point uses a **certificate-based HTTPS** web service to help secure network communication with clients. Clients must trust this certificate.

Azure Resource Manager

Starting in version 1806, create a cloud distribution point using an **Azure Resource Manager deployment**. Azure Resource Manager is a modern platform for managing all solution resources as a single entity, called a resource group. When deploying a cloud distribution point with Azure Resource Manager, the site uses Azure Active Directory (Azure AD) to authenticate and create the necessary cloud resources. This modernized deployment doesn't require the classic Azure management certificate.

> **NOTE**
> This feature doesn't enable support for Azure Cloud Service Providers (CSP). The cloud distribution point deployment with Azure Resource Manager continues to use the classic cloud service, which the CSP doesn't support. For more information, see available Azure services in Azure CSP.

Starting in Configuration Manager version 1902, Azure Resource Manager is the only deployment mechanism for new instances of the cloud distribution point. Existing deployments continue to work.

In Configuration Manager version 1810 and earlier, the cloud distribution point wizard still provides the option for a **classic service deployment** using an Azure management certificate. To simplify the deployment and management of resources, use the Azure Resource Manager deployment model for all new cloud distribution points. If possible, redeploy existing cloud distribution points through Resource Manager.

> **IMPORTANT**
> Starting in version 1810, the classic service deployment in Azure is deprecated for use in Configuration Manager. This version is the last to support creation of these Azure deployments. This functionality will be removed in a future Configuration Manager version.

Configuration Manager doesn't migrate existing classic cloud distribution points to the Azure Resource Manager

deployment model. Create new cloud distribution points using Azure Resource Manager deployments, and then remove classic cloud distribution points.

Hierarchy design

Where you create the cloud distribution point depends upon which clients need to access the content. Starting in version 1806, there are three types of cloud distribution points:

- Azure Resource Manager deployment: Create this type at a primary site or the central administration site.
- Classic service deployment: Create this type only at a primary site.
- The cloud management gateway can also serve content to clients. This functionality reduces the required certificates and cost of Azure VMs. For more information, see Plan for cloud management gateway.

To determine whether to include cloud distribution points in boundary groups, consider the following behaviors:

- Internet-based clients don't rely on boundary groups. They only use internet-facing distribution points or cloud distribution points. If you're only using cloud distribution points to service these types of clients, then you don't need to include them in boundary groups.
- If you want clients on your internal network to use a cloud distribution point, then it needs to be in the same boundary group as the clients. Clients prioritize cloud distribution points last in their list of content sources, because there's a cost associated with downloading content out of Azure. So a cloud distribution point is typically used as a fallback source for intranet-based clients. If you want a cloud-first design, then design your boundary groups to meet this business requirement. For more information, see Configure boundary groups.

Even though you install cloud distribution points in specific regions of Azure, clients aren't aware of the Azure regions. They randomly select a cloud distribution point. If you install cloud distribution points in multiple regions, and a client receives more than one in the content location list, the client might not use a cloud distribution point from the same Azure region.

Backup and recovery

When you use a cloud distribution point in your hierarchy, use the following information to help you plan for backup and recovery:

- When you use the **Backup Site Server** maintenance task, Configuration Manager automatically includes the configurations for the cloud distribution point.
- Back up and save a copy of the server authentication certificate. If you use the classic service deployment in Azure, also back up and save a copy of the Azure management certificate. When you restore the Configuration Manager primary site to a different server, you must reimport the certificates.

Requirements

- You need an **Azure subscription** to host the service.
  - An **Azure administrator** needs to participate in the initial creation of certain components, depending upon your design. This persona doesn't require permissions in Configuration Manager.
- The site server requires **internet access** to deploy and manage the cloud service.
- When using the **Azure Resource Manager** deployment method, integrate Configuration Manager with Azure AD for **Cloud Management**. Azure AD *user discovery* isn't required.
- A **server authentication certificate**. For more information, see the Certificates section below.
  - To reduce complexity, use a public certificate provider for the server authentication certificate. When doing so, you also need a **DNS CNAME alias** for clients to resolve the name of the cloud service.

- In Configuration Manager version 1810 or earlier, if using the Azure classic deployment method, you need an **Azure management certificate**. For more information, see the Certificates section below.

  > **TIP**
  > Starting with Configuration Manager version 1806, use the **Azure Resource Manager** deployment model. It doesn't require this management certificate.
  >
  > The classic deployment method is deprecated as of version 1810.

- Set the client setting, **Allow access to cloud distribution points**, to **Yes** in the **Cloud Services** group. By default, this value is set to **No**.
- Client devices require **internet connectivity**, and must use **IPv4**.

Specifications

- The cloud distribution point supports all Windows versions listed in Supported operating systems for clients and devices.
- An administrator distributes the following types of supported software content:
  - Applications
  - Packages
  - OS upgrade packages
  - Third-party software updates

  > **IMPORTANT**
  > While the Configuration Manager console doesn't block the distribution of Microsoft software updates to a cloud distribution point, you're paying Azure costs to store content that clients don't use. Internet-based clients always get Microsoft software update content from the Microsoft Update cloud service. Don't distribute Microsoft software updates to a cloud distribution point.

- Starting in version 1806, configure a pull-distribution point to use a cloud distribution point as a source. For more information, see About source distribution points.

Deployment settings

- When you deploy a task sequence with the option to **Download content locally when needed by running task sequence**, the management point doesn't include a cloud distribution point as a content location. Deploy the task sequence with the option to **Download all content locally before starting task sequence** for clients to use a cloud distribution point.
- A cloud distribution point doesn't support package deployments with the option to **Run program from distribution point**. Use the deployment option to **Download content from distribution point and run locally**.

Limitations

- You can't use a cloud distribution point for PXE or multicast-enabled deployments.
- A cloud distribution point doesn't support App-V streaming applications.
- You can't prestage content on a cloud distribution point. The distribution manager of the primary site that manages the cloud distribution point transfers all content.

- You can't configure a cloud distribution point as a pull-distribution point.

Cost

> **IMPORTANT**
> The following cost information is for estimating purposes only. Your environment may have other variables that affect the overall cost of using a cloud distribution point.

Configuration Manager includes the following options to help control costs and monitor data access:

- Control and monitor the amount of content that you store in a cloud service. For more information, see Monitor cloud distribution points.
- Configure Configuration Manager to alert you when thresholds for client downloads meet or exceed monthly limits. For more information, see Data transfer threshold alerts.
- To help reduce the number of data transfers from cloud distribution points by clients, use one of the following peer caching technologies:
  - Configuration Manager peer cache
  - Windows BranchCache
  - Windows 10 Delivery Optimization

    For more information, see Fundamental concepts for content management.

Components

A cloud distribution point uses the following Azure components, which incur charges to the Azure subscription account:

> **TIP**
> Starting in version 1806, the cloud management gateway can also serve content to clients. This functionality reduces the cost by consolidating the Azure VMs. For more information, see Cost for cloud management gateway.

Virtual machine

- The cloud distribution point uses Azure Cloud Services as platform as a service (PaaS). This service uses virtual machines (VMs) that incur compute costs.
- Each cloud distribution point service uses two Standard A0 VMs.
- See the Azure pricing calculator to help determine potential costs.

  > **NOTE**
  > Virtual machine costs vary by region.

Outbound data transfer

- Any dataflows into Azure are free (ingress or upload). Distributing content from the site to the cloud distribution point is uploading to Azure.
- Charges are based on data flowing out of Azure (egress or download). Cloud distribution point dataflows out of Azure consist of the software content that clients download.
- For more information, see Monitor cloud distribution points.

- See the Azure bandwidth pricing details to help determine potential costs. Pricing for data transfer is tiered. The more you use, the less you pay per gigabyte.

Content storage

- Internet-based clients get Microsoft software update content from the Microsoft Update cloud service at no charge. Don't distribute software update deployment packages with Microsoft software updates to a cloud distribution point. Otherwise, you'll incur data storage costs for content that clients never use.
- Cloud distribution points use the following standard blob storage depending upon the deployment model:
  - An Azure Resource Manager deployment use Azure locally redundant storage (LRS). This change reduces the cost of the storage account. The classic deployment wasn't using the additional features of GRS. For more information, see Locally redundant storage.
  - A classic deployment with Configuration Manager version 1810 or earlier uses Azure geo-redundant storage (GRS). For more information, see Geo-redundant storage.

Other costs

- Each cloud service has a dynamic IP address. Each distinct cloud distribution point uses a new dynamic IP address. Adding additional VMs per cloud service doesn't increase these addresses.

Ports and data flow

There are two primary data flows for the cloud distribution point:

- The site server connects to Azure to set up the cloud distribution point service
- A client connects to the cloud distribution point to download content

Site server to Azure

You don't need to open any inbound ports to your on-premises network. The site server initiates all communication with Azure and the cloud distribution point to deploy, update, and manage the cloud service. The site server needs to create outbound connections to the Microsoft cloud. This action is equivalent to installing the distribution point site system role on a specific site.

Client to cloud distribution point

You don't need to open any inbound ports to your on-premises network. Internet-based clients communicate directly with the Azure service. Clients on your internal network that use a cloud distribution point need to connect to the Microsoft cloud.

For more information on content location priority and when intranet-based clients use a cloud distribution point, see Content source priority.

When a client uses a cloud distribution point as a content location:

1. The management point gives the client an access token along with the list of content sources. This token is valid for 24 hours, and gives the client access to the cloud distribution point.
2. The management point responds to the client's location request with the **Service FQDN** of the cloud distribution point. This property is the same as the common name of the server authentication certificate.

   If you're using your domain name, for example, WallaceFalls.contoso.com, then the client first tries to resolve this FQDN. You need a CNAME alias in your domain's internet-facing DNS for clients to resolve the Azure service name, for example: WallaceFalls.cloudapp.net.
3. The client next resolves the Azure service name, for example, WallaceFalls.cloudapp.net, to a valid IP address. This response should be handled by Azure's DNS.
4. The client connects to the cloud distribution point. Azure load balances the connection to one of the VM

instances. The client authenticates itself using the access token.

5. The cloud distribution point authenticates the client's access token, and then gives the client the exact content location in Azure storage.
6. If the client trusts the cloud distribution point's server authentication certificate, it connects to Azure storage to download the content.

Performance and scale

As with any distribution point design, consider the following factors:

- Number of concurrent client connections
- The size of the content that clients download
- The length of time allowed to meet your business requirements

Depending upon your topology design, if clients have the option of more than one cloud distribution point for any given content, then they naturally randomize across those cloud services. If you only distribute a certain piece of content to a single cloud distribution point, and a large number of clients try to download this content at the same time, this activity puts higher load on that single cloud distribution point. Adding an additional cloud distribution point also includes a separate Azure storage service. For more information on how the client communicates with the cloud distribution point components and downloads content, see Ports and data flow.

The cloud distribution point uses two Azure VMs as the front end to the Azure storage. This default deployment meets most customer's needs. In some extreme circumstances, with a large number of concurrent client connections (for example, 150,000 clients), the processing capacity of the Azure VMs can't keep up with the client requests. You can't resize the Azure VMs used for the cloud distribution point. While you can't configure the number of VM instances for the cloud distribution point in Configuration Manager, if necessary, reconfigure the cloud service in the Azure portal. Either manually add more VM instances, or configure the service to automatically scale.

> **IMPORTANT**
> When you update Configuration Manager, the site redeploys the cloud service. If you manually reconfigure the cloud service in the Azure portal, the number of instances resets to the default of two.

The Azure storage service supports 500 requests per second for a single file. Performance testing of a single cloud distribution point supported distribution of a single 100-MB file to 50,000 clients in 24 hours.

Certificates

Depending upon your cloud distribution point design, you need one or more digital certificates.

General information

Certificates for cloud distribution points support the following configurations:

- 4096-bit key length
- Version 3 certificates. For more information, see CNG certificates overview.
- Starting in version 1802, when you configure Windows with the following policy: **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**
- Starting in version 1802, support for TLS 1.2. For more information, see Cryptographic controls technical reference.

Server authentication certificate

This certificate is required for all cloud distribution point deployments.

For more information, see CMG server authentication certificate, and the following subsections, as necessary:

- CMG trusted root certificate to clients
- Server authentication certificate issued by public provider
- Server authentication certificate issued from enterprise PKI

The cloud distribution point uses this type of certificate in the same way as the cloud management gateway. Clients also need to trust this certificate. To reduce complexity, Microsoft recommends using a certificate issued by a public provider.

Unless you use a wildcard certificate, don't reuse the same certificate. Each instance of the cloud distribution point and cloud management gateway requires a unique server authentication certificate.

For more information on creating this certificate from a PKI, see Deploy the service certificate for cloud distribution points.

Azure management certificate

This certificate is required for classic service deployments. It isn't required for Azure Resource Manager deployments.

> **IMPORTANT**
>
> Starting with Configuration Manager version 1806, use the **Azure Resource Manager** deployment model. It doesn't require this management certificate.
>
> The classic deployment method is deprecated as of version 1810.
>
> Starting in Configuration Manager version 1902, Azure Resource Manager is the only deployment mechanism for new instances of the cloud distribution point. This certificate isn't required in Configuration Manager version 1902 or later.

If using the Azure classic deployment method with Configuration Manager version 1810 or earlier, you need an **Azure management certificate**. For more information, see the Azure management certificate section of the cloud management gateway certificates article. The Configuration Manager site server uses this certificate to authenticate with Azure to create and manage the classic deployment.

To reduce complexity, use the same Azure management certificate for all classic deployments of cloud distribution points and cloud management gateways, across all Azure subscriptions and all Configuration Manager sites.

Frequently asked questions (FAQ)

Does a client need a certificate to download content from a cloud distribution point?

A client authentication certificate isn't required. The client does need to trust the server authentication certificate used by the cloud distribution point. If this certificate is issued by a public certificate provider, then most Windows devices already include trusted root certificates for these providers. If you issued a server authentication certificate from your organization's PKI, then your clients need to trust the issuing certificates in the entire chain. This chain includes the root certificate authority, and any intermediate certificate authorities. Depending upon your PKI design, this certificate can introduce additional complexity to the deployment of the cloud distribution point. To avoid this complexity, Microsoft recommends using a public certificate provider that your clients already trust.

Can my on-premises clients use a cloud distribution point?

Yes. If you want clients on your internal network to use a cloud distribution point, then it needs to be in the same boundary group as the clients. Clients prioritize cloud distribution points last in their list of content sources, because there's a cost associated with downloading content out of Azure. Thus, a cloud distribution point is typically used as a fallback source for intranet-based clients. If you want a cloud-first design, then design your

boundary groups accordingly. For more information, see Configure boundary groups.

Do I need Azure ExpressRoute?

Azure ExpressRoute lets you extend your on-premises network into the Microsoft cloud. ExpressRoute, or other such virtual network connections aren't required for the Configuration Manager cloud distribution point.

If your organization uses ExpressRoute, isolate the Azure subscription for the cloud distribution point from the subscription that uses ExpressRoute. This configuration ensures that the cloud distribution point isn't accidentally connected in this manner.

Do I need to maintain the Azure virtual machines?

No maintenance is required. The design of the cloud distribution point uses Azure platform as a service (PaaS). Using the subscription you provide, Configuration Manager creates the necessary VMs, storage, and networking. Azure secures and updates the virtual machines. These VMs aren't a part of your on-premises environment, as is the case with infrastructure as a service (IaaS). The cloud distribution point is a PaaS that extends your Configuration Manager environment into the cloud. For more information, see Security advantages of a PaaS cloud service model.

Does the cloud distribution point use Azure CDN?

The Azure Content Delivery Network (CDN) is a global solution for rapidly delivering high-bandwidth content by caching the content at strategically placed physical nodes across the world. For more information, see What is Azure CDN?.

The Configuration Manager cloud distribution point currently doesn't support Azure CDN.

Next steps

Install cloud distribution points

Use a pull-distribution point with Configuration Manager

6/19/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

When you distribute content to a standard distribution point in the Configuration Manager console, the site server pushes the content to the distribution point. A pull-distribution point gets content by downloading it from a source location like a client.

When you distribute content to many distribution points, pull-distribution points help reduce the processing load on the site server. They can also speed the content transfer to each server. Normally the distribution manager component on the site server sends content to each distribution point. Instead, the site offloads the process of transferring the content to the pull-distribution points.

You configure individual distribution points to be pull-distribution points. For each pull-distribution point, specify one or more source distribution points from which it can get content. A pull-distribution point can only download content from a distribution point that you specify as a source distribution point.

When you distribute content to a pull-distribution point in the console, the site server sends it a notification. The pull-distribution point then downloads the content from a source distribution point. A pull-distribution point manages the content transfer by downloading from a distribution point that already has a copy of the content.

Pull-distribution points support the same configurations and functionality as typical distribution points. For example, a pull-distribution point supports:

- Multicast and PXE configurations
- Content validation
- On-demand content distribution
- HTTP or HTTPS communications from clients
- The same certificate options as other distribution points
- Manage individually or as a member of a distribution point group

> **IMPORTANT**
> Although a pull-distribution point supports communications over HTTP and HTTPS, when you use the Configuration Manager console, you can only specify source distribution points that are configured for HTTP. You can use the Configuration Manager SDK to specify a source distribution point that is configured for HTTPS.

Configure a pull-distribution point when you install the distribution point. After you create a distribution point, configure it as a pull-distribution point by editing the role properties. For more information on how to enable a distribution point as a pull-distribution point, see Pull-distribution point.

Remove the configuration to be a pull-distribution point by editing the properties of the distribution point. When you remove the configuration as a pull-distribution point, it returns to normal operation. The site server manages future content transfers to the distribution point.

Distribution process

When you distribute content to a pull-distribution point, the following sequence of events occurs:

- Once you distribute content to a pull-distribution point in the console, the Package Transfer Manager

component on the site server checks the site database to confirm if the content is available on a source distribution point. If it can't confirm that the content is on a source distribution point for the pull-distribution point, it repeats the check every 20 minutes until the content is available.

- When the Package Transfer Manager confirms that the content is available, it notifies the pull-distribution point to download the content. If this notification fails, it retries based on the Software Distribution component **Retry settings** for pull-distribution points. When the pull-distribution point receives this notification, it tries to download the content from its source distribution points.
- While the pull-distribution point downloads the content, the Package Transfer Manager polls the status based on the Software Distribution component **Status polling settings** for pull-distribution points. When the pull-distribution point completes the download of content, it submits this status to a management point.

Configure site component settings

When you use a pull-distribution point, review and configure the following site component settings:

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. Select the site. In the ribbon, click **Configure Site Components**, and select **Software Distribution**.
3. Switch to the **Pull Distribution Point** tab.
4. In the **Retry settings** group, review the following values:
   - **Number of retries**: The number of times that the Package Transfer Manager tries to notify the pull-distribution point to download the content. After it tries this number of times, the Package Transfer Manager cancels the transfer. This value is 30 by default.
   - **Delay before retrying (minutes)**: The number of minutes that the Package Transfer Manager waits between attempts. This value is 20 by default.
5. In the **Status polling settings** group, review the following values:
   - **Number of polls**: The number of times that the Package Transfer Manager contacts the pull-distribution point to retrieve the job status. If it tries this number of times before the job completes, the Package Transfer Manager cancels the transfer. This value is 72 by default.
   - **Delay before retrying (minutes)**: The number of minutes that the Package Transfer Manager waits between attempts. This value is 60 by default.

> **NOTE**
> When the Package Transfer Manager cancels a job because it exceeds the number of polling retries, the pull-distribution point continues to download the content. When it finishes, the pull-distribution point sends the appropriate status message, and the console reflects the new status.

Limitations

- You can't configure a cloud distribution point as a pull-distribution point.
- You can't configure the distribution point role on a site server as a pull-distribution point.
- The prestage content configuration overrides the pull-distribution point configuration. If you turn on the option to **Enable this distribution point for prestaged content** on a pull-distribution point, it waits for the content. It doesn't pull content from the source distribution point. Like a standard distribution point enabled for prestaged content, it doesn't receive content from the site server. For more information, see

Prestaged content.

- A pull-distribution point doesn't use schedule or rate limit configurations. When you configure a previously installed distribution point to be a pull-distribution point, configurations for schedule and rate limits are saved, but not used. If you later remove the pull-distribution point configuration, the schedule and rate limit configurations are implemented as previously configured.

  > **NOTE**
  > The **Schedule** and **Rate Limits** tabs aren't visible in the properties of the distribution point.

- Pull-distribution points don't use the settings on the **General** tab of the **Software Distribution Component Properties** for each site. These settings include **Concurrent distribution** and **Multicast retry**.
- To transfer content from a source distribution point in a remote forest, install the Configuration Manager client on the pull-distribution point. Also configure a network access account that can access the source distribution point. Starting in version 1806, if you enable the site option to **Use Configuration Manager-generated certificates for HTTP site systems**, then you don't need a network access account.
- If the pull-distribution point is also a Configuration Manager client, the client version must be the same as the Configuration Manager site that installs the pull-distribution point. The pull-distribution point uses the CCMFramework that is common to both the pull-distribution point and the Configuration Manager client.

About source distribution points

When you configure the pull-distribution point, specify one or more source distribution points:

- The wizard only displays distribution points that qualify to be source distribution points.
- A pull-distribution point can be specified as a source distribution point for another pull-distribution point.
- Only distribution points that support HTTP can be specified as source distribution points when you use the Configuration Manager console.
- Use the Configuration Manager SDK to specify a source distribution point that's configured for HTTPS. To use a source distribution point that's configured for HTTPS, install the Configuration Manager client on the pull-distribution point.
- Starting in version 1806, if your remote offices have a better connection to the internet, or to reduce load on your WAN links, use a cloud distribution point in Microsoft Azure as the source. The pull-distribution point needs internet access to communicate with Microsoft Azure. The content must be distributed to the source cloud distribution point.

  > **NOTE**
  > This feature does incur charges to your Azure subscription for data storage and network egress. For more information, see the Cost of using a cloud distribution point.

> **TIP**
> When a pull-distribution point downloads content from a source distribution point, that pull-distribution point is counted as a client in the **Client Accessed (Unique)** column of the **Distribution point usage summary** report.

Source priorities

- Assign a separate priority to each source distribution point, or assign multiple source distribution points to the same priority.
- The priority determines the order in which the pull-distribution point requests content from its source distribution points.
- Pull-distribution points initially contact a source distribution point with the lowest value for priority. If there are multiple source distribution points with the same priority, the pull-distribution point randomly selects one of the sources with that priority.
- If the content isn't available on a selected source, the pull-distribution point then tries to download the content from another distribution point with that same priority.
- If none of the distribution points with a given priority has the content, the pull-distribution point tries to download the content from a source distribution point with the next priority level. It continues this search until the content is located.
- If none of the assigned source distribution points have the content, the pull-distribution point waits for 30 minutes, and then starts the process again.

Inside the pull-distribution point

- To manage the transfer of content, pull-distribution points use the **CCMFramework** component. The Configuration Manager client includes this component.
- When you enable the pull-distribution point, the site installs **pulldp.msi**. This installer also adds the CCMFramework component. The framework doesn't require the Configuration Manager client.
- After the pull-distribution point is installed, it primarily uses the **CCMExec** service to function.
- When the pull-distribution point transfers content, it uses the **Background Intelligent Transfer Service** (BITS) built into Windows. A pull-distribution point doesn't require that you install the BITS Extension for IIS Server.
- For operational details, see the following log files on the pull-distribution point:
  - **DataTransferService.log**
  - **PullDP.log**

See also

Fundamental concepts for content management

The content library in Configuration Manager

8/1/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The content library is a single-instance store of content in Configuration Manager. The site uses it to reduce the overall size of the combined body of content that you distribute. The content library stores all content files for software deployments, for example: software updates, applications, and OS deployments.

- The site automatically creates and maintains a copy of the content library on each site server and each distribution point.
- Before Configuration Manager adds content files to the site server or copies the files to distribution points, it verifies whether each content file is already in the content library.
- If the content file is available, Configuration Manager doesn't copy the file. It instead associates the existing content file with the application or package.

On distribution point servers, configure the following options:

- One or more disk drives on which you want to create the content library.
- A priority for each drive that you use.

Configuration Manager copies content files to the drive with the highest priority until that drive contains less than a minimum amount of free space that you specify.

- You configure the drive settings during the distribution point installation.
- You can't configure the drive settings in the distribution point properties after the installation has finished.

For more information about how to configure the drive settings for the distribution point, see Manage content and content infrastructure.

> **IMPORTANT**
> To move the content library to a different location on a distribution point after the installation, use the **Content Library Transfer** tool in the Configuration Manager tools. For more information, see the Content Library Transfer tool.

About the content library on the central administration site

By default, Configuration Manager creates a content library on the central administration site when the site is installed. The content library is placed on the drive of the site server that has the most free disk space. Because you can't install a distribution point on the central administration site, you can't prioritize the drives for use by the content library. Similar to the content library on other site servers and on distribution points, when the drive that contains the content library runs out of available disk space, the content library automatically spans to the next available drive.

Configuration Manager uses the content library on the central administration site in the following scenarios:

- You create content on the central administration site
- You migrate content from another Configuration Manager site, and assign the central administration site as the site that manages that content

> **NOTE**
> When you create content at a primary site and then distribute it to a different primary site or a secondary site below a different primary site, the central administration site temporarily stores that content in the scheduler inbox on the central administration site but doesn't add that content to its content library.

Use the following options to manage the content library on the central administration site:

- To prevent the content library from being installed on a specific drive, create an empty file named **no_sms_on_drive.sms**. Copy it to the root of the drive before the content library is created.
- After the content library has been created, use the **Content Library Transfer** tool from the Configuration Manager tools to manage the location of the content library. For more information, see the Content Library Transfer tool.

> **NOTE**
> Cloud distribution points don't use single-instance storage. The site encrypts packages before sending to Azure, and each package has a unique encrypted key. Even if two files were identical, the encrypted versions wouldn't be the same.

Configure a remote content library for the site server

Starting in version 1806, to configure site server high availability or to free up hard drive space on your central administration or primary site servers, relocate the content library to another storage location. Move the content library to another drive on the site server, a separate server, or fault-tolerant disks in a storage area network (SAN). A SAN is recommended, because it's highly available, and provides elastic storage that grows or shrinks over time to meet your changing content requirements. For more information, see High availability options.

A remote content library is a prerequisite for site server high availability.

> **NOTE**
> This action only moves the content library on the site server. It doesn't impact the location of the content library on distribution points.

> **TIP**
> Also plan for managing package source content, which is external to the content library. Every software object in Configuration Manager has a package source on a network share. Consider centralizing all sources to a single share, but make sure this location is redundant and highly available.
>
> If you move the content library to the same storage volume as your package sources, you can't mark this volume for data deduplication. While the content library supports data deduplication, the package sources volume doesn't support it. For more information, see Data deduplication.

Prerequisites

- The site server computer account needs **Full control** permissions to the network path to which you're moving the content library. This permission applies to both the share and the file system. No components are installed on the remote system.
- The site server can't have the distribution point role. The distribution point also uses the content library, and this role doesn't support a remote content library. After moving the content library, you can't add the distribution point role to the site server.

> **IMPORTANT**
> Don't reuse a shared network location between multiple sites. For example, don't use the same path for both a central administration site and a child primary site. This configuration has the potential to corrupt the content library, and require you to rebuild it.

Process to manage the content library

1. Create a folder in a network share as the target for the content library. For example, `\\server\share\folder`.

   > **WARNING**
   > Don't reuse an existing folder with content. For example, don't use the same folder as your package sources. Before copying the content library, Configuration Manager removes any existing content from the location you specify.

2. In the Configuration Manager console, switch to the **Administration** workspace. Expand **Site Configuration**, select the **Sites** node, and select the site. On the **Summary** tab at the bottom of the details pane, notice a new column for the **Content Library**.

3. Select **Manage Content Library** on the ribbon.

4. In the Manage Content Library window, the **Current Location** field shows the local drive and path. Enter a valid network path for the **New Location**. This path is the location to which the site moves the content library. It must include a folder name that already exists on the share, for example, `\\server\share\folder`. Select **OK**.

5. Note the **Status** value in the Content Library column on the Summary tab of the details pane. It updates to show the site's progress in moving the content library.

   - While **In progress**, the **Move Progress (%)** value displays the percentage complete.

     > **NOTE**
     > If you have a large content library, you may see `0%` progress in the console for a while. For example, with a 1 TB library, it has to copy 10 GB before it shows `1%`. Review **distmgr.log**, which shows the number of files and bytes copied. Starting in version 1810, the log file also shows an estimated time remaining.

   - If there's an error state, the status displays the error. Common errors include**access denied** or **disk full**.

   - When complete it displays **Complete**.

     See the **distmgr.log** for details. For more information, see Site server and site system server logs.

For more information on this process, see Flowchart - Manage content library.

The site actually *copies* the content library files to the remote location. This process doesn't delete the content library files at the original location on the site server. To free up space, an administrator must manually delete these original files.

If the original content library spans two drives, it's merged into a single folder at the new destination.

Starting in version 1810, during the copy process, the **Despooler** and **Distribution manager** components don't process new packages. This action makes sure that content isn't added to the library while it's moving. Regardless, schedule this change during a system maintenance.

If you need to move the content library back to the site server, repeat this process, but enter a local drive and path

for the **New Location**. It must include a folder name that already exists on the drive, for example, `D:\SCCMContentLib`. When the original content still exists, the process quickly moves the configuration to the location local to the site server.

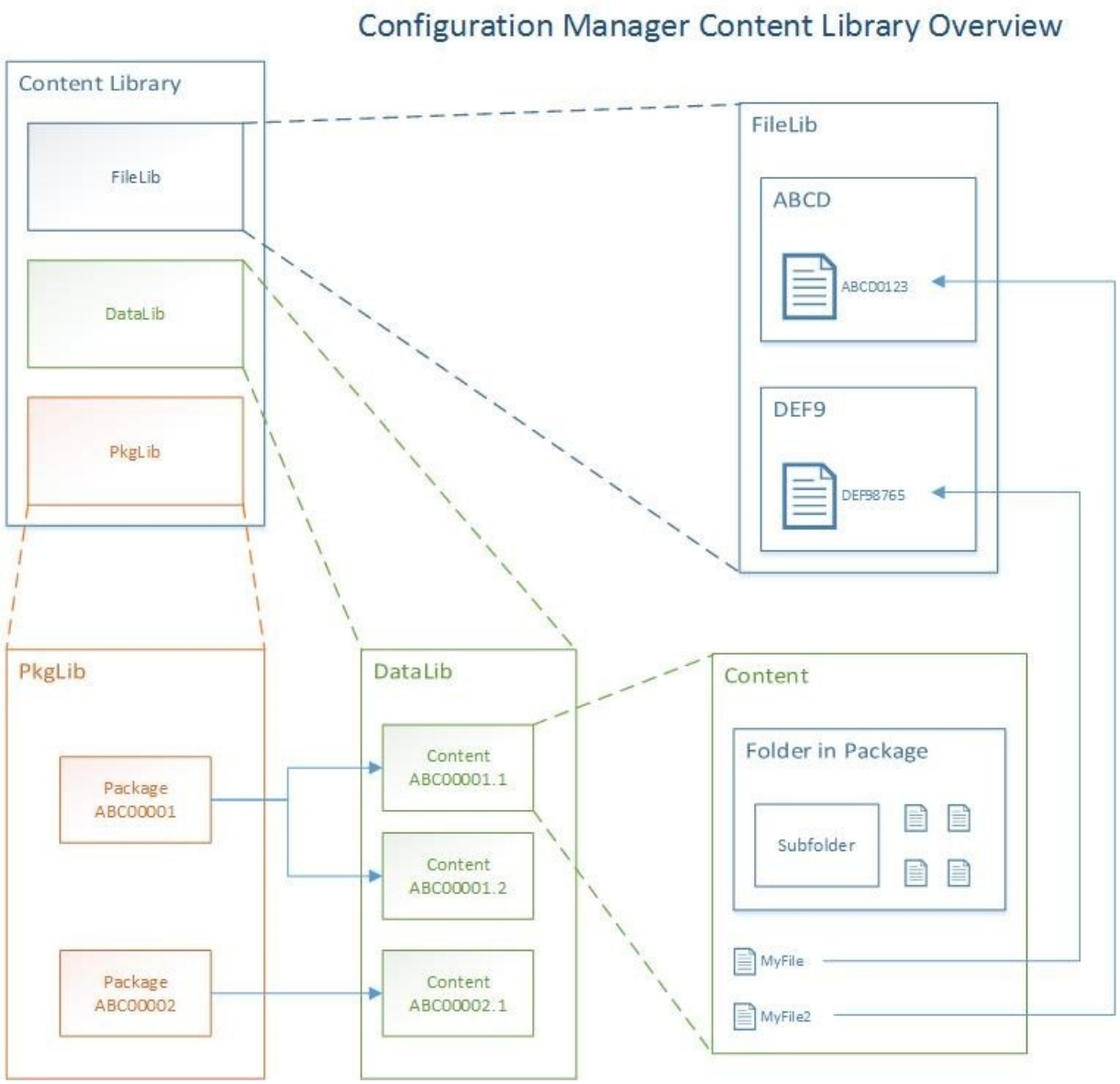
> **TIP**
> To move the content to another drive on the site server, use the **Content Library Transfer** tool. For more information, see the Content Library Transfer tool.

Inside the content library

> **WARNING**
> The following section is provided for informational purposes only. Don't alter, add, or remove any files or folders in the content library. Doing so could corrupt packages, contents, or the content library as a whole. If you suspect any missing, corrupt, or otherwise invalid data, use the validation feature in the Configuration Manager console to detect such issues. Then redistribute the affected content to correct the issues.

By default, the content library is stored on the root of a drive in a folder called **SCCMContentLib**. This folder is shared by default as **SCCMContentLib$**. The folder and share have restricted permissions to prevent accidental damage. All changes should be made from the Configuration Manager console. Within this folder are the following objects:

- The package library (**PkgLib** folder): Information about what packages are present on the distribution point.
- The data library (**DataLib** folder): Information about the original structure of the packages.
- The file library (**FileLib** folder): The original files in the package. This folder is typically what uses the bulk of the storage.



TIP

Use the **Content Library Explorer** tool from the Configuration Manager tools to browse the contents of the content library. You can't use this tool to modify the contents. It provides insight into what's present, as well as allowing validation and redistribution. For more information, see the Content Library Explorer.

Package library

The package library folder, **PkgLib**, includes one file for each package distributed to the distribution point. The file name is the package ID, for example, `ABC00001.INI`. In this file under the `[Packages]` section is a list of content IDs that are part of the package, as well as other information such as the version. For example, **ABC00001** is a legacy package at version **1**. The content ID in this file is `ABC00001.1`.

Data library

The data library folder, **DataLib**, includes one file and one folder for each of the contents in each package. For example, this file and folder are named `ABC00001.1.INI` and `ABC00001.1`, respectively. The file includes information for validation. The folder recreates the folder structure from the original package.

The files in the data library are replaced by INI files with the name of the original file in the package. For example, `MyFile.exe.INI`. These files include information about the original file, such as the size, time modified, and the hash. Use the first four characters of the hash to locate the original file in the file library. For example, the hash in MyFile.exe.INI is **DEF98765**, and the first four characters are **DEF9**.

File library

If the content library spans across multiple drives, the package files could be in the file library folder, **FileLib**, on any of these drives.

Locate a specific file using the first four characters from the hash found in the data library. Inside the file library folder are many folders, each with a four-character name. Find the folder that matches the first four characters from the hash. Once you find this folder, it includes one or more sets of three files. These files share the same name, but one has the extension INI, one has the extension SIG, and one has no file extension. The original file is the one with no extension whose name is equal to the hash from the data library.

For example, folder **DEF9** includes `DEF98765.INI`, `DEF98765.SIG`, and `DEF98765`. `DEF98765` is the original `MyFile.exe`. The INI file includes a list of "users" or content IDs that share the same file. The site doesn't remove a file unless all of these contents are also removed.

Drive spanning

The content library can be spanned across multiple drives. You choose these drives when creating the distribution point. By default, Configuration Manager automatically chooses the drives when spanning the content library.

When you choose the drives, select a primary and secondary drive. The site stores all metadata on the primary drive. It only spans the file library across to the secondary drive. The folder's share name for secondary drives includes the drive letter. For example, if D: and E: are secondary drives for the content library, the share names are **SCCMContentLibD$** and **SCCMContentLibE$**.

If you chose the **Automatic** option, Configuration Manager selects the drive with the most available free space as its primary drive. It stores all of the metadata on this drive. The site only spans the file library across to secondary drives.

You specify a reserve space amount during configuration. Configuration Manager attempts to use a secondary disk once the best available disk has only this reserve space amount left free. Each time a new drive is selected for use, the drive with the most available free space is selected.

You can't specify that a distribution point should use all drives except for a specific set. Prevent this behavior by creating an empty file on the root of the drive, called `NO_SMS_ON_DRIVE.SMS`. Place this file before Configuration Manager selects the drive for use. If Configuration Manager detects this file on the root of the drive, it doesn't use the drive for the content library.

Troubleshooting

The following tips may help you troubleshoot issues with the content library:

- Review the logs on the site server (**distmgr.log** and **PkgXferMgr.log**) and the distribution point (**smsdpprov.log**) for any pointers to the failures.
- Use the Content Library Explorer tool.
- Check for file locks by other processes, such as antivirus software. Exclude the content library on all drives from automatic antivirus scans, as well as the temporary staging directory, **SMS_DP$**, on each drive.
- To see if there are any hash mismatches, validate the package from the Configuration Manager console.
- As a last option, redistribute the content. This action should resolve most issues.

Flowchart - Manage content library

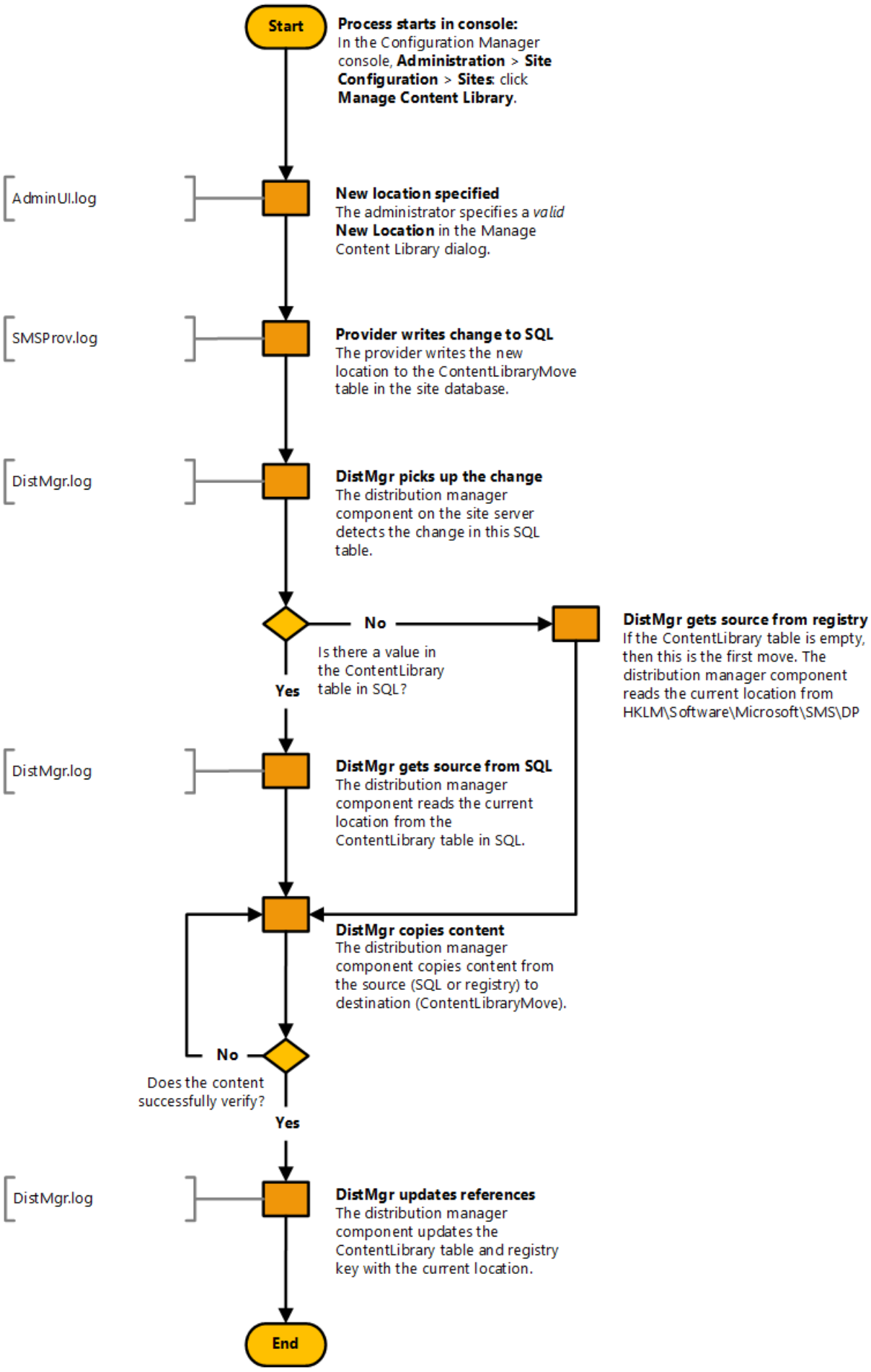
2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This flowchart diagram shows the process by which the site moves the content library to a remote location. For more information, see the following articles:

- The content library
- Site server high availability

Manage Content Library



Content library cleanup tool

2/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the content library cleanup command-line tool to remove content that's no longer associated with any package or application on a distribution point. This type of content is called *orphaned content*. This tool replaces older versions of similar tools released for past Configuration Manager products.

The tool only affects the content on the distribution point that you specify when you run the tool. The tool can't remove content from the content library on the site server.

Find **ContentLibraryCleanup.exe** in `CD.Latest\SMSSETUP\TOOLS\ContentLibraryCleanup` on the site server.

Requirements

- Only run the tool against a single distribution point at a time.
- Run it directly on the computer that hosts the distribution point to cleanup, or remotely from another computer.
- The user account that runs the tool must have permissions the same as the **Full Administrator** security role in Configuration Manager.

Modes of operation

Run the tool in the following two modes: What-if and Delete.

> **TIP**
> Start with the *what-if* mode. When you're satisfied with the results, then run the tool in *delete* mode.

What-if mode

If you don't specify the `/delete` parameter, the tool runs in what-if mode. This mode identifies the content that would be deleted from the distribution point.

- When run in this mode, the tool doesn't delete any data.
- The tool writes to the log file information about the content that it would delete. You're not prompted to confirm each potential deletion.

Delete mode

When you run the tool with the `/delete` parameter, the tool runs in delete mode.

- When run in this mode, orphaned content that it finds on the specified distribution point can be deleted from the distribution point's content library.
- Before deleting each file, confirm that the tool should delete it. Select **Y** for yes, **N** for no, or **Yes to all** to skip further prompts and delete all orphaned content.

Log file

When the tool runs in either mode, it automatically creates a log. It names the log file with the following information:

- The mode the tool runs in
- The name of the distribution point
- The date and time of operation

When the tool finishes, it automatically opens the log file in Windows.

By default, the tool writes the log file to the temp folder of the user account that runs the tool. This location is on the computer where you run the tool, which isn't always the target of the tool. Use the `/log` parameter to redirect the log file to another location, including a network share.

Run the tool

To run the tool:

1. Open a command prompt as an administrator. Change directory to the folder that contains **ContentLibraryCleanup.exe**.
2. Enter a command line that includes the required command-line parameters, and any optional parameters you want to use.

Command-line parameters

Use these command-line parameters in any order.

Required parameters

PARAMETER	DETAILS
`/dp <distribution point FQDN>`	Specify the fully qualified domain name (FQDN) of the distribution point to clean.
`/ps <primary site FQDN>`	*Required* only when cleaning content from a distribution point at a secondary site. The tool connects to the parent primary site to run queries against the SMS Provider. These queries let the tool determine what content should be on the distribution point. It can then identify the orphaned content to remove. This connection to the parent primary site must be made for distribution points at a secondary site because the required details aren't available directly from the secondary site.
`/sc <primary site code>`	*Required* only when cleaning content from a distribution point at a secondary site. Specify the site code of the parent primary site.

Example: Scan and log what content it would delete (what-if)

```
ContentLibraryCleanup.exe /dp server1.contoso.com
```

Example: Scan and log content for a DP at a secondary site

```
ContentLibraryCleanup.exe /dp server1.contoso.com /ps siteserver1.contoso.com /sc ABC
```

Optional parameters

PARAMETER	DETAILS

PARAMETER	DETAILS
`/delete`	Use this parameter when you're ready to delete content from the distribution point. It prompts you before it deletes content. When you don't use this parameter, the tool logs results about what content it would delete. Without this parameter, it doesn't actually delete any content from the distribution point.
`/q`	This parameter runs the tool in a quiet mode that suppresses all prompts. These prompts include when it deletes content. It also doesn't automatically open the log file.
`/ps <primary site FQDN>`	Optional only when cleaning content from a distribution point at a primary site. Specify the FQDN of the primary site that the distribution point belongs to.
`/sc <primary site code>`	Optional only when cleaning content from a distribution point at a primary site. Specify the site code of the primary site that the distribution point belongs to.
`/log <log file directory>`	Specify the location where the tool writes the log file. This location can be a local drive or a network share. When you don't use this parameter, the tool places the log file in the user's temp directory on the computer where the tool runs.

Example: Delete content

```
ContentLibraryCleanup.exe /dp server1.contoso.com /delete
```

Example: Delete content without prompts

```
ContentLibraryCleanup.exe /q /dp server1.contoso.com /delete
```

Example: Log to local drive

```
ContentLibraryCleanup.exe /dp server1.contoso.com /log C:\Users\Administrator\Desktop
```

Example: Log to network share

```
ContentLibraryCleanup.exe /dp server1.contoso.com /log \\server\share
```

Known issue

When any package or deployment has failed, or is in progress, the tool might return the following error:

```
System.InvalidOperationException: This content library cannot be cleaned up right now because package
<packageID> is not fully installed.
```

There's no workaround for this issue. The tool can't reliably identify orphaned files when content is in progress or has failed to deploy. The tool won't allow you to clean up content until you resolve that issue.

Peer cache for Configuration Manager clients

9/11/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use peer cache to help manage deployment of content to clients in remote locations. Peer cache is a built-in Configuration Manager solution that enables clients to share content with other clients directly from their local cache.

> **NOTE**
> Configuration Manager doesn't enable this optional feature by default. You must enable this feature before using it. For more information, see Enable optional features from updates.

Overview

Definitions:

- **Peer cache client**: Any Configuration Manager client that downloads content from a peer
- **Peer cache source**: A Configuration Manager client that you enable for peer cache, and that has content to share with other clients

Use client settings to enable clients to be peer cache sources. You don't need to enable peer cache clients. When you enable clients to be peer cache sources, the management point includes them in the list of content location sources. For more information on this process, see Operations.

A peer cache source must be a member of the current boundary group of the peer cache client. The management point doesn't include peer cache sources from a neighbor boundary group in the list of content sources it provides the client. It only includes distribution points from a neighbor boundary group. For more information about current and neighbor boundary groups, see Boundary groups.

The Configuration Manager client uses peer cache to serve to other clients every type of content in the cache. This content includes Office 365 files and express installation files.

Peer cache doesn't replace the use of other solutions like Windows BranchCache or Delivery Optimization. Peer cache works along with other solutions. These technologies give you more options for extending traditional content deployment solutions such as distribution points. Peer cache is a custom solution with no reliance on BranchCache. If you don't enable or use BranchCache, peer cache still works.

> **NOTE**
> Starting in version 1802, Windows BranchCache is always enabled on deployments. The setting to **Allow clients to share content with other clients on the same subnet** is removed. If the distribution point supports it, and it's enabled in client settings, clients use BranchCache. For more information, see Configure BranchCache.

Operations

To enable peer cache, deploy the client settings to a collection. Then members of that collection act as a peer cache source for other clients in the same boundary group.

- A client that operates as a peer content source submits a list of available cached content to its management

point using state messages.

> **NOTE**
> See State messages in Configuration Manager for the list of applicable peer content source state messages specifcally those with with state message IDs of 7200, 7201, 7202, and 7203.

- Another client in the same boundary group makes a content location request to the management point. The server returns the list of potential content sources. This list includes each peer cache source that has the content and is online. It also includes the distribution points and other content source locations in that boundary group. For more information, see Content source priority.
- As usual, the client that's seeking the content selects one source from the provided list. The client then attempts to get the content.

Starting in version 1806, boundary groups include additional settings to give you more control over content distribution in your environment. For more information, see Boundary group options for peer downloads.

> **NOTE**
> If the client falls back to a neighbor boundary group for content, the management point doesn't add the peer cache sources from the neighbor boundary group to the list of potential content source locations.

Choose only clients best suited as peer cache sources. Evaluate client suitability based on attributes such as chassis type, disk space, and network connectivity. For more information that can help you select the best clients to use for peer cache, see this blog by a Microsoft consultant.

Limited access to a peer cache source

A peer cache source rejects requests for content when it meets any of the following conditions at the time a peer requests content:

- Low battery mode
- Processor load exceeds 80%
- Disk I/O has an *AvgDiskQueueLength* that exceeds 10
- There are no more available connections to the computer

> **TIP**
> Configure these settings using the client configuration server WMI class for the peer source feature (*SMS_WinPEPeerCacheConfig*) in the Configuration Manager SDK.

When the peer cache source rejects a request for the content, the peer cache client continues to seek content from its list of content source locations.

Requirements

- Peer cache supports all Windows versions listed as supported in Supported operating systems for clients and devices. Non-Windows operating systems aren't supported as peer cache sources or peer cache clients.
- A peer cache source must be a domain-joined Configuration Manager client. However, a client that's not domain-joined can get content from a domain-joined peer cache source.

- Clients can only download content from peer cache sources in their current boundary group.
- A network access account isn't required with the following exception:
  - Configure a network access account in the site when a peer cache-enabled client runs a task sequence from Software Center, and it reboots to a boot image. When the device is in Windows PE, it uses the network access account to get content from the peer cache source.
  - When required, the peer cache source uses the network access account to authenticate download requests from peers. This account requires only domain user permissions for this purpose.
- With version 1802 and prior, the client's last heartbeat discovery submission determines the current boundary of a peer cache source. A client that roams to a different boundary group might still be a member of its former boundary group for the purposes of peer cache. This behavior results in a client being offered a peer cache source that isn't in its immediate network location. Don't enable roaming clients as a peer cache source.

  > **IMPORTANT**
  > Starting in version 1806, Configuration Manager is more efficient at determining if a peer cache source has roamed to another location. This behavior makes sure the management point offers it as a content source to clients in the new location and not the old location. If you're using the peer cache feature with roaming peer cache sources, after updating the site to version 1806, also update all peer cache sources to the latest client version. The management point doesn't include these peer cache sources in the list of content locations until they are updated to at least version 1806.

- Before attempting to download content, the management point first validates that the peer cache source is online. This validation happens via the "fast channel" for client notification, which uses TCP port 10123.

> **NOTE**
> To take advantage of new Configuration Manager features, first update clients to the latest version. While new functionality appears in the Configuration Manager console when you update the site and console, the complete scenario isn't functional until the client version is also the latest.

Peer cache client settings

For more information about the peer cache client settings, see Client cache settings.

For more information on configuring these settings, see How to configure client settings.

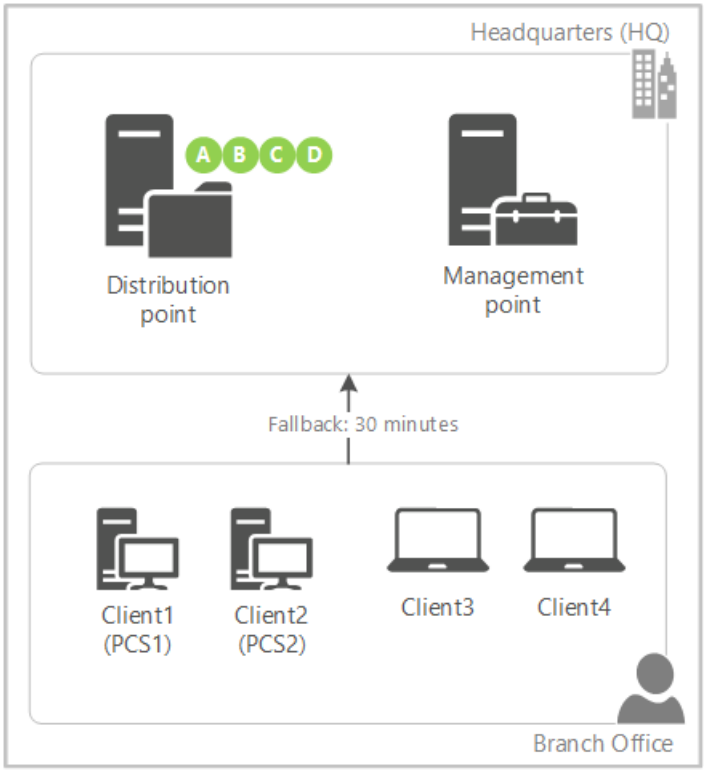
On peer cache-enabled clients that use the Windows Firewall, Configuration Manager configures the firewall ports that you specify in client settings.

Partial download support

Starting in version 1806, client peer cache sources can now divide content into parts. These parts minimize the network transfer to reduce WAN utilization. The management point provides more detailed tracking of the content parts. It tries to eliminate more than one download of the same content per boundary group.

Example scenario

Contoso has a single primary site with two boundary groups: Headquarters (HQ) and Branch Office. There's a 30-minute fallback relationship between the boundary groups. The management point and distribution point for the site are only in the HQ boundary. The branch office location has no local distribution point. Two of the four clients at the branch office are configured as peer cache sources.



1. You target a deployment with content to all four clients in the branch office. You only distributed the content to the distribution point.
2. Client3 and Client4 don't have a local source for the deployment. The management point instructs the clients to wait 30 minutes before falling back to the remote boundary group.
3. Client1 (PCS1) is the first peer cache source to refresh policy with the management point. Because this client is enabled as a peer cache source, the management point instructs it to immediately start downloading part A from the distribution point.
4. When Client2 (PCS2) contacts the management point, as part A is already in progress but not yet complete, the management point instructs it to immediately start downloading part B from the distribution point.
5. PCS1 finishes downloading part A, and immediately notifies the management point. As part B is already in progress but not yet complete, the management point instructs it to start downloading part C from the distribution point.
6. PCS2 finishes downloading part B, and immediately notifies the management point. The management point instructs it to start downloading part D from the distribution point.
7. PCS1 finishes downloading part C, and immediately notifies the management point. The management point informs it that there are no more parts available from the remote distribution point. The management point instructs it to download part B from its local peer, PCS2.
8. This process continues until both client peer cache sources have all of the parts from each other. The management point prioritizes parts from the remote distribution point before instructing the peer cache sources to download parts from local peers.
9. Client3 is the first to refresh policy after the 30-minute fallback period expires. It now checks back with the management point, which informs the client of new local sources. Instead of downloading the content in full from the distribution point across the WAN, it downloads the content in full from one of the client peer cache sources. Clients prioritize local peer sources.

> **NOTE**
> If the number of client peer cache sources is greater than the number of content parts, then the management point instructs the additional peer cache sources to wait for fallback like a normal client.

Configure partial download

1. Set up boundary groups and peer cache sources per normal.
2. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select **Sites**. Click **Hierarchy Settings** in the ribbon.
3. On the **General** tab, enable the option to **Configure client peer cache sources to divide content into parts**.
4. Create a required deployment with content.

   > **NOTE**
   > This functionality only works when the client downloads content in the background, such as with a required deployment. On-demand downloads, such as when the user installs an available deployment in Software Center, behaves as usual.

To see them handling the download of content in parts, examine the **ContentTransferManager.log** on the client peer cache source and the **MP_Location.log** on the management point.

Guidance for cache management

Peer cache relies on the Configuration Manager client cache to share content. Consider the following points for managing the client cache in your environment:

- The Configuration Manager client cache isn't like the content library on a distribution point. While you manage the content that you distribute to a distribution point, the Configuration Manager client automatically manages the content in its cache. There are settings and methods to help control what content is in the cache of a peer cache source. For more information, see Configure the client cache for Configuration Manager clients.
- Normal cache size and maintenance applies to peer cache sources. For more information, see Configure client cache size. Consider the size of larger content such as OS upgrade packages or Windows 10 express update files. Compare your need for this content against the available disk space on peer cache sources.
- The peer cache source client updates the last referenced time of content in the cache when a peer downloads it. The client uses this timestamp when it automatically maintains its cache, removing older content first. So it should wait to remove content that peer cache clients more frequently download, if at all.
- If necessary, during an OS deployment task sequence, use the **SMSTSPreserveContent** variable to keep content in the client cache. For more information, see Task sequence variables.
- If necessary, when creating the following software, use the option to **Persist content in the client cache**:
  - Applications
  - Packages
  - OS images
  - OS upgrade packages
  - Boot images

Monitoring

To help you understand the use of peer cache, view the **Client Data Sources** dashboard. For more information, see Client data sources dashboard.

Also use reports to view peer cache use. In the console, go to the **Monitoring** workspace, expand **Reporting**, and select the **Reports** node. The following reports all have a type of **Software Distribution Content**:

1. **Peer cache source content rejection**: How often the peer cache sources in a boundary group reject a content request.

   > **NOTE**
   >
   > **Known issue**: When drilling down on results like *MaxCPULoad* or *MaxDiskIO*, you might receive an error that suggests the report or details can't be found. To work around this issue, use the other two reports that directly show the results.

2. **Peer cache source content rejection by condition**: Shows rejection details for a specified boundary group or rejection type.

   > **NOTE**
   >
   > **Known issue**: You can't select from available parameters and instead must enter them manually. Enter the values for *Boundary Group Name* and *Rejection Type* as seen in the **Peer cache source content rejection** report. For example, for *Rejection Type* you might enter *MaxCPULoad* or *MaxDiskIO*.

3. **Peer cache source content rejection details**: Show the content that the client was requesting when rejected.

   > **NOTE**
   >
   > **Known issue**: You can't select from available parameters and instead must enter them manually. Enter the value for *Rejection Type* as displayed in the **Peer cache source content rejection** report. Then enter the *Resource ID* for the content source about which you want more information.
   >
   > To find the Resource ID of the content source:
   >
   > 1. Find the computer name that displays as the *Peer cache source* in the results of the **Peer cache source content rejection by condition** report.
   > 2. Go to the **Assets and Compliance** workspace, select the **Devices** node, and search for that computer's name. Use the value from the Resource ID column.

Package Transfer Manager in System Center Configuration Manager

9/11/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

In a System Center Configuration Manager site, the Package Transfer Manager is a component of the SMS_Executive service that manages the transfer of content from a site server computer to remote distribution points in a site. (A remote distribution point is one that is not located on the site server computer.) The Package Transfer Manager does not support configurations by the admin, but understanding how it operates can help you plan your content management infrastructure. It can also help you resolve problems with content distribution.

When you distribute content to one or more remote distribution points at a site, the **Distribution Manager** creates a content transfer job. It then notifies the Package Transfer Manager on primary and secondary site servers to transfer the content to the remote distribution points.

Package Transfer Manager logs its actions in the **pkgxfermgr.log** file on the site server. The log file is the only location where you can view the activities of the Package Transfer Manager.

> **NOTE**
> In previous versions of Configuration Manager, the Distribution Manager manages the transfer of content to a remote distribution point. Distribution Manager also manages the transfer of content between sites. With the System Center Configuration Manager, Distribution Manager continues to manage the transfer of content between two sites. However, the Package Transfer Manager now manages the transfer of content to large numbers of distribution points. This helps to increase the overall performance of content deployment both between sites and to distribution points within a site.

To transfer content to a standard distribution point, Package Transfer Manager operates the same as the Distribution Manager operates in previous versions of Configuration Manager. That is, it actively manages the transfer of files to each remote distribution point. However, to distribute content to a pull-distribution point, the Package Transfer Manager notifies the pull-distribution point that content is available. The pull-distribution point then takes over the transfer process.

The following information describes how Package Transfer Manager manages the transfer of content to standard distribution points, and to distribution points configured as pull-distribution points:

1. **Admin deploys content to one or more distribution points at a site.**
   - **Standard distribution point:** Distribution Manager creates a content transfer job for that content.
   - **Pull-distribution point:** Distribution Manager creates a content transfer job for that content.
2. **Distribution Manager runs preliminary checks.**
   - **Standard distribution point:** Distribution Manager runs a basic check to confirm that each distribution point is ready to receive the content. After this check, Distribution Manager notifies Package Transfer Manager to start the transfer of content to the distribution point.
   - **Pull-distribution point:** Distribution Manager starts Package Transfer Manager, which then notifies the pull-distribution point that there is a new content transfer job. Distribution Manager does not check on the status of remote distribution points that are pull-distribution points, because each pull-distribution point manages its own content transfers.

3. **Package Transfer Manager prepares to transfer content.**

   - **Standard distribution point:** Package Transfer Manager examines the single instance content store of each specified remote distribution point. The purpose of this is to identify any files that are already on that distribution point. Then, Package Transfer Manager queues up for transfer only those files that are not already present.

     > **NOTE**
     > To copy each file in the distribution to the distribution point, even if the files are already present in the single instance store of the distribution point, use the **Redistribute** action for content.

   - **Pull-distribution point:** For each pull-distribution point in the distribution, Package Transfer Manager checks the pull-distribution points source distribution points, to confirm if the content is available.

     - When the content is available on at least one source distribution point, Package Transfer Manager sends a notification to that pull-distribution point. The notification directs that distribution point to begin the process of transferring content. The notification includes file names and sizes, attributes, and hash values.

     - When the content is not yet available, Package Transfer Manager does not send a notification to the distribution point. Instead, it repeats the check every 20 minutes until the content is available. Then, when the content is available, Package Transfer Manager sends the notification to that pull-distribution point.

     > **NOTE**
     > For the pull-distribution point to copy each file in the distribution to the distribution point, even if the files are already present in the single instance store of the pull-distribution point, use the **Redistribute** action for content.

4. **Content begins to transfer.**

   - **Standard distribution point:** Package Transfer Manager copies files to each remote distribution point. During the transfer to a standard distribution point:

     - By default, Package Transfer Manager can simultaneously process three unique packages, and distribute them to five distribution points in parallel. Collectively, these are called **Concurrent distribution settings**. To set up concurrent distribution, in the **Software Distribution Component Properties** for each site, go to the **General** tab.

     - Package Transfer Manager uses the scheduling and network bandwidth configurations of each distribution point when transferring content to that distribution point. To configure these settings, in the **Properties** of each remote distribution point, go to the **Schedule** and **Rate Limits** tabs. For more information, see Manage content and content infrastructure for System Center Configuration Manager.

   - **Pull-distribution point:** When a pull-distribution point receives a notification file, the distribution point begins the process to transfer the content. The transfer process runs independently on each pull-distribution point:

     a. The pull-distribution identifies the files in the content distribution that it does not already have in its single instance store, and prepares to download that content from one of its source distribution points.

b. Next, the pull-distribution point checks with each of its source distribution points, in order, until it locates a source distribution point that has the content available. When the pull-distribution point identifies a source distribution point with the content, it begins the download of that content.

> **NOTE**
>
> The process to download content by the pull-distribution point is the same as that used by Configuration Manager clients. For the transfer of content by the pull-distribution point, concurrent transfer settings aren't used. Scheduling and throttling options that you configure for standard distribution points aren't used either.

5. **Content transfer completes.**

- **Standard distribution point:** After the Package Transfer Manager is done transferring files to each designated remote distribution point, it verifies the hash of the content on the distribution point. Then it notifies Distribution Manager that the distribution is complete.
- **Pull-distribution point:** After the pull-distribution point completes the content download, the distribution point verifies the hash of the content. Then it submits a status message to the site management point to indicate success. If, after 60 minutes, this status is not received, the Package Transfer Manager wakes up again. It checks with the pull-distribution point to confirm whether the pull-distribution point has downloaded the content. If the content download is in progress, the Package Transfer Manager sleeps for another 60 minutes before it checks with the pull-distribution point again. This cycle continues until the pull-distribution point completes the content transfer.

Manage network bandwidth for content

9/11/2019 • 5 minutes to read • Edit Online

To help you manage network bandwidth that is used for the content management process of System Center Configuration Manager, you can use built-in controls for scheduling and throttling. You can also use prestaged content. The following sections describe these options in more detail.

Scheduling and throttling

When you create a package, change the source path for the content, or update content on the distribution point, the files are copied from the source path to the content library on the site server. Then, the content is copied from the content library on the site server to the content library on the distribution points. When content source files are updated, and the source files have already been distributed, Configuration Manager retrieves only the new or updated files, and then sends them to the distribution point.

You can use scheduling and throttling controls for site-to-site communication, and for communication between a site server and a remote distribution point. If network bandwidth is limited even after you set up the scheduling and throttling controls, you might consider prestaging the content on the distribution point.

In Configuration Manager, you can set up a schedule and specify throttling settings on remote distribution points that determine when and how content distribution is performed. Each remote distribution point can have different configurations that help address network bandwidth limitations from the site server to the remote distribution point. The controls for scheduling and throttling to the remote distribution point are similar to the settings for a standard sender address. In this case, the settings are used by a new component, called Package Transfer Manager.

Package Transfer Manager distributes content from a site server, as a primary site or secondary site, to a distribution point that is installed on a site system. The throttling settings are specified on the **Rate Limits** tab, and the scheduling settings are specified on the **Schedule** tab, for a distribution point that is not on a site server. The time settings are based on the time zone from the sending site, not the distribution point.

> **IMPORTANT**
> The **Rate Limits** and **Schedule** tabs are displayed only in the properties for distribution points that are not installed on a site server.

For more information, see Install and configure distribution points for System Center Configuration Manager.

Prestaged content

You can prestage content to add the content files to the content library on a site server or distribution point, before you distribute the content. Because the content files are already in the content library, they do not transfer over the network when you distribute the content. You can prestage content files for applications and packages.

In the Configuration Manager console, select the content that you want to prestage, and then use the **Create Prestaged Content File Wizard**. This creates a compressed, prestaged content file that contains the files and associated metadata for the content. Then, you can manually import the content at a site server or distribution point. Note the following points:

- When you import the prestaged content file on a site server, the content files are added to the content library on the site server, and then registered in the site server database.

- When you import the prestaged content file on a distribution point, the content files are added to the content library on the distribution point. A status message is sent to the site server that informs the site that the content is available on the distribution point.

You can optionally configure the distribution point as **prestaged** to help manage content distribution. Then, when you distribute content, you can choose whether you want to:

- Always prestage the content on the distribution point.
- Prestage the initial content for the package, and then use the standard content distribution process when there are updates to the content.
- Always use the standard content distribution process for the content in the package.

Determine whether to prestage content

Consider prestaging content for applications and packages in the following scenarios:

- **To address the issue of limited network bandwidth from the site server to a distribution point.** If scheduling and throttling aren't enough to satisfy your concerns about bandwidth, consider prestaging the content on the distribution point. Each distribution point has the **Enable this distribution point for prestaged content** setting that you can choose in the distribution point properties. When you enable this option, the distribution point is identified as a prestaged distribution point, and you can choose how to manage the content on a per-package basis.

  The following settings are available in the properties for an application, package, driver package, boot image, operating system installer, and image. These settings let you choose how content distribution is managed on remote distribution points that are identified as prestaged:

  - **Automatically download content when packages are assigned to distribution points**: Use this option when you have smaller packages, and the scheduling and throttling settings provide enough control for content distribution.
  - **Download only content changes to the distribution point**: Use this option when you expect future updates to the content in the package to be generally smaller than the initial package. For example, you might prestage an application like Microsoft Office, because the initial package size is over 700 MB and is too large to send over the network. However, content updates to this package might be less than 10 MB, and are acceptable to distribute over the network. Another example might be driver packages, where the initial package size is large, but incremental driver additions to the package might be small.
  - **Manually copy the content in this package to the distribution point**: Use this option when you have large packages, with content such as an operating system, and you never want to use the network to distribute the content to the distribution point. When you select this option, you must prestage the content on the distribution point.

  > **IMPORTANT**
  > The preceding options are applicable on a per-package basis, and are only used when a distribution point is identified as prestaged. Distribution points that have not been identified as prestaged ignore these settings. In this case, content always is distributed over the network from the site server to the distribution points.

- **To restore the content library on a site server.** When a site server fails, information about packages and applications that is contained in the content library is restored to the site database as part of the restore process, but the content library files are not restored as part of the process. If you do not have a file system backup to restore the content library, you can create a prestaged content file from another site that contains the packages and applications that you have to have. You can then extract the prestaged content file on the

recovered site server. For more information about site server backup and recovery, see Backup and recovery for System Center Configuration Manager.

Security and privacy for content management in Configuration Manager

2/12/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article contains security and privacy information for content management in Configuration Manager.

Security best practices for content management

Advantages and disadvantages of HTTPS or HTTP for intranet distribution points

For distribution points on the intranet, consider the advantages and disadvantages of using HTTPS and HTTP. In most scenarios, using HTTP and package access accounts for authorization provides more security than using HTTPS with encryption but without authorization. However, if you have sensitive data in your content that you want to encrypt during transfer, use HTTPS.

- **When you use HTTPS for a distribution point**, Configuration Manager doesn't use package access accounts to authorize access to the content, but the content is encrypted when it's transferred over the network.
- **When you use HTTP for a distribution point**, you can use package access accounts for authorization, but the content isn't encrypted when it's transferred over the network.

Starting in version 1806, consider enabling **Enhanced HTTP** for the site. This feature allows clients to use Azure Active Directory authentication to securely communicate with an HTTP distribution point. For more information, see Enhanced HTTP.

Protect the client authentication certificate file

If you use a PKI client authentication certificate rather than a self-signed certificate for the distribution point, protect the certificate file (.pfx) with a strong password. If you store the file on the network, secure the network channel when you import the file into Configuration Manager.

When you require a password to import the client authentication certificate that the distribution point uses to communicate with management points, this configuration helps to protect the certificate from an attacker. Use Server Message Block (SMB) signing or IPsec between the network location and the site server to prevent an attacker from tampering with the certificate file.

Remove the distribution point role from the site server

By default, Configuration Manager setup installs a distribution point on the site server. Clients don't have to communicate directly with the site server. To reduce the attack surface, assign the distribution point role to other site systems and remove it from the site server.

Secure content at the package access level

The distribution point share allows read access to all users. To restrict which users can access the content, use package access accounts when the distribution point is configured for HTTP. This configuration doesn't apply to cloud distribution points, which don't support package access accounts. For more information, see Package access accounts.

Configure IIS on the distribution point role

If Configuration Manager installs IIS when you add a distribution point site system role, remove HTTP redirection or IIS Management Scripts and Tools when the distribution point installation is complete. The distribution point doesn't require HTTP redirection or IIS Management Scripts and Tools. To reduce the attack surface, remove these

role services for the web server role. For more information about the role services for the web server role for distribution points, see Site and site system prerequisites.

Set package access permissions when you create the package

Because changes to the access accounts on the package files become effective only when you redistribute the package, set the package access permissions carefully when you first create the package. This configuration is important when the package is large or distributed to many distribution points, and when the network bandwidth capacity for content distribution is limited.

Implement access controls to protect media that contains prestaged content

Prestaged content is compressed but not encrypted. An attacker could read and modify the files that are downloaded to devices. Configuration Manager clients reject content that's tampered with, but they still download it.

Import prestaged content with ExtractContent

Only import prestaged content by using the ExtractContent.exe command-line tool. To avoid tampering and elevation of privileges, use only the authorized command-line tool that comes with Configuration Manager.

Secure the communication channel between the site server and the package source location

Use IPsec or SMB signing between the site server and the package source location when you create applications and packages. This configuration helps to prevent an attacker from tampering with the source files.

Remove default virtual directories for custom website with the distribution point role

If you change the site configuration option to use a custom website rather than the default website after installing a distribution point role, remove the default virtual directories. When you switch from the default website to a custom website, Configuration Manager doesn't remove the old virtual directories. Remove the following virtual directories that Configuration Manager originally created under the default website:

- SMS_DP_SMSPKG$
- SMS_DP_SMSSIG$
- NOCERT_SMS_DP_SMSPKG$
- NOCERT_SMS_DP_SMSSIG$

For cloud distribution points, protect your Azure subscription details and certificates

When you use cloud distribution points, protect the following high-value items:

- The user name and password for your Azure subscription
- The Azure management certificate
- The cloud distribution point service certificate

Store the certificates securely. If you browse to them over the network when you configure the cloud distribution point, use IPsec or SMB signing between the site system server and the source location.

For service continuity, monitor the expiry date of the cloud distribution point certificates

Configuration Manager doesn't warn you when the imported certificates for the cloud distribution point are about to expire. Monitor the expiry dates independently from Configuration Manager. Make sure that you renew and then import the new certificates before the expiry date. This action is important if you acquire a server authentication certificate from an external, public provider, because you might need additional time to acquire a renewed certificate.

If either certificate expires, Cloud Services Manager generates the status message ID **9425**. The CloudMgr.log file contains an entry to indicate that the certificate **is in expired state**, with the expiry date also logged in UTC.

Security considerations for content management

Consider the following points when planning for content management:

- Clients don't validate content until after it's downloaded.

  Configuration Manager clients validate the hash on content only after it's downloaded to their client cache. If an attacker tampers with the list of files to download or with the content itself, the download process can take up considerable network bandwidth, only for the client to then discard the content when it encounters the invalid hash.

- When you use cloud distribution points, access to the content is automatically restricted to your enterprise. You can't restrict it further to selected users or groups.

- When you use cloud distribution points, clients are authenticated by the management point and then use a Configuration Manager token to access cloud distribution points. The token is valid for eight hours. This behavior means that if you block a client because it's no longer trusted, it can continue to download content from a cloud distribution point until the validity period of this token has expired. At this point, the management point won't issue another token for the client because the client is blocked.

  To avoid a blocked client from downloading content within this eight-hour window, stop the cloud service. In the Configuration Manager console, go to the **Administration** workspace, expand **Cloud Services**, and select the **Cloud Distribution Points** node.

Privacy information for content management

Configuration Manager doesn't include any user data in content files, although an administrative user might choose to do this action.

See also

- Fundamental concepts for content management
- Security and privacy for application management
- Security and privacy for software updates
- Security and privacy for OS deployment

Data transfers between sites

8/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager uses *file-based replication* and *database replication* to transfer different types of information between sites. Learn about how Configuration Manager moves data between sites, and how you can manage the transfer of data across your network.

Types of replication

File-based replication

Configuration Manager uses file-based replication to transfer file-based data between sites in your hierarchy. This data includes applications and packages that you want to deploy to distribution points in child sites. It also handles unprocessed discovery data records that the site transfers to its parent site and then processes.

For more information, see File-based replication.

Database replication

Configuration Manager database replication uses SQL Server to transfer data. It uses this method to merge changes in its site database with the information from the database at other sites in the hierarchy.

For more information, see Database replication.

For help with troubleshooting SQL replication, see Troubleshoot SQL replication.

See also

Monitor replication

File-based replication

8/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager uses file-based replication to transfer file-based data between sites in your hierarchy. This data includes applications and packages that you want to deploy to distribution points in child sites. It also handles unprocessed discovery data records that the site transfers to its parent site and then processes.

File-based communication between sites uses the *server message block* (SMB) protocol on TCP/IP port 445. To control the amount of data the site transfers across the network, specify bandwidth throttling and pulse mode. Use schedules to control when to send data across the network.

Routes

The following information can help you set up and use file replication routes.

File replication route

Each file replication route identifies a destination site to which a site transfers file-based data. Each site supports one file replication route to a specific destination site.

To manage a file replication route, go to the **Administration** workspace. Expand the **Hierarchy Configuration** node, and then select **File Replication**.

You can change the following settings for file replication routes:

File replication account

This account connects to the destination site, and writes data to that site's **SMS_Site** share. The receiving site processes the data written to this share. By default, when you add a site to the hierarchy, Configuration Manager assigns the new site server's computer account as its file replication account. It then adds this account to the destination site's `SMS_SiteToSiteConnection_<sitecode>` group. This group is local to the computer that grants access to the SMS_Site share. You can change this account to be a Windows user account. If you change the account, make sure you add the new account to the destination site's `SMS_SiteToSiteConnection_<sitecode>` group.

> **NOTE**
> Secondary sites always use the computer account of the secondary site server as the **File Replication Account**.

Schedule

Set the schedule for each file replication route. This action restricts the type of data and time when data can transfer to the destination site.

Rate limits

Specify rate limits for each file replication route. This action controls the network bandwidth the site uses when it transfers data to the destination site:

- **Pulse mode**: Specify the size of the data blocks that the site sends to the destination site. You can also specify a time delay between sending each data block. Use this option when you must send data across a low-bandwidth network connection to the destination site.

  For example, you have constraints to send 1 KB of data every five seconds, but not 1 KB every three seconds. This constraint is regardless of the speed of the link or its usage at a given time.

- **Limited to maximum transfer rates by hour**: The site sends data to a destination site by using only the percentage of time that you specify. Configuration Manager doesn't identify the network's available bandwidth. It divides the time it can send data into slices of time. It then sends the data in a short block of time, which is followed by blocks of time when it doesn't send data.

  For example, you set the maximum rate to **50%**. Configuration Manager transmits data for an amount of time followed by an equal period of time when it doesn't send any data. It doesn't manage the actual size of the data block that it sends. The site only manages the amount of time during which it sends data.

  Caution

  By default, a site can use up to three **concurrent sendings** to transfer data to a destination site. When you enable rate limits for a file replication route, it limits the **concurrent sendings** to that site to one. This behavior applies even when the **Limit available bandwidth (%)** is set to **100%**. For example, if you use the default settings for the sender, this reduces the transfer rate to the destination site to be one-third of the default capacity.

Routes between secondary sites

Configure a file replication route between two secondary sites to route file-based content between those sites.

Sender

Each site has one sender. The sender manages the network connection from one site to a destination site. It can establish connections to multiple sites at the same time. To connect to a site, the sender uses the file replication route to the site and identifies the account it uses to establish the network connection. The sender also uses this account to write data to the destination site's SMS_Site share.

By default, the sender writes data to a destination site by using multiple **concurrent sendings**, or a *thread*. Each thread can transfer a different file-based object to the destination site. When the sender begins to send an object, it continues to write blocks of data for that object until it sends the entire object. After it sends all the data for the object, a new object can begin to send on that thread.

To manage the sender for a site, go to the **Administration** workspace, and expand the **Site Configuration** node. Select the **Sites** node, and then select **Properties** for the site you want to manage. Switch to the **Sender** tab to change the sender settings.

You can change the following settings for a sender:

Maximum concurrent sendings

By default, each site uses five concurrent sendings (threads). Three threads are available for use when it sends data to any one destination site. When you increase this number, you can increase the throughput of data between sites. More threads mean that Configuration Manager can transfer more files at the same time. Increasing this number also increases the demand for network bandwidth between sites.

Retry settings

By default, each site retries a problem connection two times, with a one-minute delay between connection attempts. You can modify the number of connection attempts the site makes, and how long to wait between attempts.

Next steps

Database replication

Database replication

8/12/2019 • 12 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager database replication uses SQL Server to transfer data. It uses this method to merge changes in its site database with the information from the database at other sites in the hierarchy.

Note the following points about database replication:

- All sites share the same information.
- When you install a site in a hierarchy, Configuration Manager automatically establishes database replication between the new site and its parent site.
- When the site installation finishes, database replication automatically starts.

When you add a new site to a hierarchy, Configuration Manager creates a generic database at the new site. The parent site creates a snapshot of the relevant data in its database. It then transfers the snapshot to the new site using file-based replication. The new site then uses the SQL Server Bulk Copy Program (BCP) to load the information into its local copy of the Configuration Manager database. After the snapshot loads, each site conducts database replication with the other site.

To replicate data between sites, Configuration Manager uses its own database replication service. The database replication service uses SQL Server change tracking to monitor the local site database for changes. It then replicates the changes to other sites by using SQL Server Service Broker (SSB). By default, this process uses TCP port 4022.

Replication groups

Configuration Manager groups data that replicates by database replication into different replication groups. Each replication group has a separate, fixed replication schedule. The site uses this schedule to determine how frequently it replicates changes to other sites.

For example, a change to a role-based administration configuration replicates quickly to other sites. This behavior makes sure that the other site can quickly enforce these changes. A lower-priority configuration change, such as a request to install a new secondary site, replicates with less urgency. It can take several minutes for a new site request to reach the destination primary site.

Settings

You can modify the following settings for database replication:

- **Database replication links**: Control when specific traffic traverses the network.
- **Distributed views**: When a central administration site (CAS) requests selected site data, it can access the data directly from the database at a child primary site.
- **Schedules**: Specify when a replication link is used, and when different types of site data replicate.
- **Summarization**: Change settings for data summarization about network traffic that traverses replication links. By default, summarization occurs every 15 minutes. It's used in reports for database replication.
- **Database replication thresholds**: Define when the site reports links as degraded or failed. You can also

configure when Configuration Manager raises alerts about replication links that have a degraded or failed status.

Types of data

Configuration Manager primarily classifies the data that it replicates as either *global data* or *site data*. When database replication occurs, the site transfers changes to global data and site data across the database replication link. Global data replicates to a parent or child site. Site data replicates only to a parent site. A third data type, *local data*, doesn't replicate to other sites. Local data is information that other sites don't require.

Global data

Global data is administrator-created objects that replicate to all sites throughout the hierarchy. Secondary sites only receive a subset of global data, as global proxy data. You create global data at the CAS and primary sites. This type includes the following data:

- Software deployments
- Software updates
- Collection definitions
- Role-based administration security scopes

Site data

Site data is operational information created by Configuration Manager primary sites and their assigned clients. Site data replicates to the CAS, but not to other primary sites. Site data is only viewable at the CAS and at the primary site where the data originates. You can only modify site data at the primary site where you created it. This type includes the following data:

- Hardware inventory
- Status messages
- Alerts
- The results of query-based collections

All site data replicates to the CAS. The CAS does administration and reporting for the entire site hierarchy.

Database replication links

When you install a new site in a hierarchy, Configuration Manager automatically creates a database replication link between the parent site and the new site. It creates a single link to connect the two sites.

To control the transfer of data across the replication link, change settings for each link. Each replication link supports separate configurations. Each database replication link includes the following controls:

- Stop the replication of selected site data from a primary site to the CAS. This action causes the CAS to access this data directly from the database of the primary site.
- Schedule selected site data to transfer from a child primary site to the CAS.
- Define the settings that determine when a database replication link has a degraded or failed status.
- Specify when to raise alerts for a failed replication link.
- Specify how frequently Configuration Manager summarizes data about the replication traffic that uses the replication link. It uses this data in reports.

To configure a database replication link, in the Configuration Manager console, go to the **Monitoring** workspace. Select the **Database Replication** node, and edit the properties for the link. This node is also in the **Administration** workspace, under the **Hierarchy Configuration** node. Edit a replication link from either the

parent site or the child site of the replication link.

> **TIP**
> You can edit database replication links from the **Database Replication** node in either workspace. However, when you use the **Database Replication** node in the **Monitoring** workspace, you can also view the status of database replication. It also provides access to the Replication Link Analyzer tool. Use this tool to help investigate problems with database replication.

For more information about how to configure replication links, see Site database replication controls. For more information about how to monitor replication, see Monitor database replication.

Distributed views

Through distributed views, when you make a request at the CAS for selected site data, it directly accesses the database at the child primary site. This direct access replaces the need to replicate site data from the primary site to the CAS. Because each replication link is independent from other replication links, you can use distributed views on the replication links that you choose. You can't use distributed views between a primary site and a secondary site.

Distributed views provide the following benefits:

- Reduce the CPU load to process database changes at the CAS and primary sites
- Reduce the amount of data that transfers across the network to the CAS
- Improve the performance of the SQL Server that hosts the CAS database
- Reduce the disk space used by the CAS database

Consider using distributed views when a primary site is closely located to the CAS on the network, the two sites are always on, and always connected. Distributed views replace the replication of the selected data between the sites with direct connections between the SQL servers at each site. The CAS makes a direct connection each time you request this data.

The site requests distributed view data in the following example scenarios:

- When you run reports or queries
- When you view information in Resource Explorer
- Collection evaluation for collections that include site data-based rules

By default, distributed views are turned off for each replication link. When you turn on distributed views, you select site data that won't replicate to the CAS across that link. The CAS accesses this data directly from the database of the child primary site that shares the link. You can configure the following types of site data for distributed views:

- **Hardware inventory** data from clients
- **Software inventory and software metering** data from clients
- **Status messages** from clients, the primary site, and all secondary sites

When you view data in the Configuration Manager console or in reports, distributed views are operationally invisible to you. When you request data that's enabled for distributed views, the CAS site database server directly accesses the child primary site's database to retrieve the information.

For example, you use a Configuration Manager console connected to the CAS. You request information about hardware inventory from two primary sites: ABC and XYZ. You only enabled hardware inventory for distributed views at site ABC. The CAS retrieves inventory information for XYZ clients from its own database. The CAS retrieves inventory information for ABC clients directly from the database at site ABC. This information appears in the Configuration Manager console or in a report without identifying the source.

If a replication link has a type of data enabled for distributed views, the child primary site doesn't replicate that data to the CAS. When you turn off distributed views for a type of data, the child primary site resumes normal data replication to the CAS. Before this data is available at the CAS, the replication groups for this data must reinitialize between the primary site and the CAS. After you uninstall a primary site that has distributed views turned on, the CAS must complete reinitialization of its data before you can access data that you enabled for distributed views on the CAS.

> **IMPORTANT**
>
> When you use distributed views on any replication link in the site hierarchy, before you uninstall any primary site, turn off distributed views for all replication links. For more information, see Uninstall a primary site that is configured with distributed views.

Prerequisites and limitations for distributed views

- Only use distributed views on replication links between the CAS and a primary site.
- The CAS must use SQL Server Enterprise edition. The primary site doesn't have this requirement.
- The CAS can have only one instance of the SMS Provider. Install that single instance on the site database server. This configuration supports Kerberos authentication. The SQL server at the CAS requires Kerberos to access the SQL server at the child primary site. There are no limitations on the SMS Provider at the child primary site.
- You can only install one reporting services point at the CAS. Install SQL Server Reporting Services on the site database server. This configuration supports Kerberos authentication. The SQL server at the CAS requires Kerberos to access the SQL server at the child primary site.
- You can't host the site database on a SQL Server cluster.
- In version 1902 and earlier, you can't host the site database on aSQL Server Always On availability group. To support this configuration, update to version 1906 or later.
- The computer account of the CAS database server requires **Read** permissions on the primary site database.

> **IMPORTANT**
>
> Distributed views and schedules for when data can replicate are mutually exclusive settings for a database replication link.

Schedule transfers of site data

To help you control the network bandwidth that's used to replicate site data from a child primary site to the CAS, schedule when a replication link is used. Then specify when different types of site data replicate. You can control when the primary site replicates status messages, inventory, and metering data. Database replication links from secondary sites don't support schedules for site data. You can't schedule the transfer of global data.

When you configure a database replication link schedule, you can restrict the transfer of selected site data from the primary site to the CAS. You can also configure different times to replicate different types of site data.

> **IMPORTANT**
>
> Distributed views and schedules for when data can replicate are mutually exclusive configurations for a database replication link.

Summarization of traffic

Each site periodically summarizes data about the network traffic that traverses database replication links for the site. The site uses summarized data in reports for database replication. Both sites on a replication link summarize the network traffic that traverses the replication link. The site database server summarizes the data. After it summarizes data, the information replicates to other sites as global data.

By default, summarization occurs every 15 minutes. To modify the frequency of summarization for network traffic, in the properties of the database replication link, edit the **Summarization interval**. The frequency of summarization affects the information that you view in reports about database replication. You can choose an interval from 5 to 60 minutes. When you increase the frequency of summarization, you increase the processing load on the SQL Server at each site on the replication link.

Database replication thresholds

Database replication thresholds define when Configuration Manager reports the status of a database replication link as either degraded or failed. By default, it sets a link as *degraded* when any one replication group fails to complete replication for 12 consecutive attempts. It sets the link as *failed* when any replication group fails to replicate in 24 consecutive attempts.

You can specify custom values for degraded or failed status. If you adjust these values, you can more accurately monitor the health of database replication across the links.

One or more replication groups can fail to replicate while other replication groups continue to successfully replicate. Plan to review the replication status of a link when it first reports as degraded.

Consider modifying the retry values for the degraded or failed status of the link in the following situations:

- There are recurring delays for specific replication groups, and their delay isn't a problem
- The network link between sites has low available bandwidth

When you increase the number of retries before the site sets the link to degraded or failed, you can eliminate false warnings for known issues. This action lets you more accurately track the status of the link.

To understand how frequently replication of that group occurs, consider the replication sync interval for each replication group. To view the **Synchronization Interval** for replication groups, go to the **Monitoring** workspace in the Configuration Manager console. In the **Database Replication** node, select the **Replication Detail** tab of a replication link.

For more information about how to monitor database replication, including how to view the replication status, see Monitor database replication.

Site database replication controls

To help you control the network bandwidth used for database replication, change the settings for each site database. The settings apply only to the site database in which you configure the settings. The settings are always used when the site replicates any data by database replication to any other site.

You can modify the following replication controls for each site database:

- The SSB port
- The period of time to wait before replication failures trigger the site to reinitialize its copy of the site database
- Compress the data that a site replicates. It only compresses the data for transfer between sites, and not for storage in the site database at either site.

To change the settings for the replication controls for a site database, in the Configuration Manager console, on the

Database Replication node, edit the properties of the site database. This node appears under the **Hierarchy Configuration** node in the **Administration** workspace, and also appears in the **Monitoring** workspace. To edit the properties of the site database, select the replication link between the sites, and then open either **Parent Database Properties** or **Child Database Properties**.

> **TIP**
>
> You can configure database replication controls from the **Database Replication** node in either workspace. However, when you use the **Database Replication** node in the **Monitoring** workspace, you can also view the status of database replication for a replication link, and access the Replication Link Analyzer tool to help you investigate problems with replication.

See also

Monitor replication

Troubleshoot SQL replication

Learn how clients find site resources and services for System Center Configuration Manager

9/11/2019 • 14 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

System Center Configuration Manager clients use a process called *service location* to locate site system servers that they can communicate with, and that provide services that clients are directed to use. Understanding how and when clients use service location to find site resources can help you configure your sites to successfully support client tasks. These configurations can require the site to interact with domain and network configurations like Active Directory Domain Services (AD DS) and DNS. Or they can require you to configure more complex alternatives.

Examples of site system roles that provide services include:

- The core site system server for clients.
- The management point.
- Additional site system servers that the client can communicate with, like distribution points and software update points.

Fundamentals of service location

A client evaluates its current network location, communication protocol preference, and assigned site when it is using service location to find a management point that it can communicate with.

A client communicates with a management point to:

- Download information about other management points for the site, so it can build a list of known management points (known as the *MP list*) for future service location cycles.
- Upload configuration details, like inventory and status.
- Download a policy that sets configurations on the client and can inform the client of software that it can or must install, and other related tasks.
- Request information about additional site system roles that provide services that the client has been configured to use. Examples include distribution points for software that the client can install, or a software update point from which to get updates.

A Configuration Manager client makes a service location request:

- Every 25 hours of continuous operation.
- When the client detects a change in its network configuration or location.
- When the **ccmexec.exe** service on the computer (the core client service) starts.
- When the client must locate a site system role that provides a required service.

When a client is attempting to find servers that host site system roles, it uses service location to find a site system role that supports the client's protocol (HTTP or HTTPS). By default, clients use the most secure method available to them. Consider the following:

- To use HTTPS, you must have a public key infrastructure (PKI) and install PKI certificates on clients and servers. For information about how to use certificates, see PKI certificate requirements for System Center Configuration Manager.

- When you deploy a site system role that uses Internet Information Services (IIS) and supports communication from clients, you must specify whether clients connect to the site system by using HTTP or HTTPS. If you use HTTP, you must also consider signing and encryption choices. For more information, see Planning for Signing and Encryption in the Plan for security in System Center Configuration Manager.

Service location and how clients determine their assigned management point

When a client is first assigned to a primary site, it selects a default management point for that site. Primary sites support multiple management points, and each client independently identifies a management point as its default management point. This default management point then becomes that client's assigned management point. (You can also use client installation commands to set the assigned management point for a client when it's installed.)

A client selects a management point to communicate with based on the client's current network location and boundary group configurations. Even though it has an assigned management point, this might not be the management point that the client uses.

> **NOTE**
> A client always uses the assigned management point for registration messages and certain policy messages, even when other communications are sent to a proxy or local management point.

You can use preferred management points. Preferred management points are management points from a client's assigned site that are associated with a boundary group that the client is using to find site system servers. A preferred management point's association with a boundary group as a site system server is similar to how distribution points or state migration points are associated with a boundary group. If you enable preferred management points for the hierarchy, when a client uses a management point from its assigned site, it will try to use a preferred management point before using other management points from its assigned site.

You can also use the information in the management point affinity blog on TechNet.com to configure management point affinity. Management point affinity overrides the default behavior for assigned management points and lets the client use one or more specific management points.

Each time a client needs to contact a management point, it checks the MP list, which it stores locally in Windows Management Instrumentation (WMI). The client creates an initial MP list when it's installed. The client then periodically updates the list with details about each management point in the hierarchy.

When the client cannot find a valid management point in its MP list, it searches the following service location sources, in order, until it finds a management point that it can use:

1. Management point
2. AD DS
3. DNS
4. WINS

After a client successfully locates and contacts a management point, it downloads the current list of management points that are available in the hierarchy, and it updates the local MP list. This applies equally to clients that are domain joined and those that are not.

For example, when a Configuration Manager client that is on the internet connects to an internet-based management point, the management point sends that client a list of available internet-based management points in the site. Similarly, clients that are domain joined or in workgroups also receive the list of management points that they might use.

A client that is not configured for the internet is not provided internet-facing-only management points.

Workgroup clients configured for the internet communicate only with internet-facing management points.

The MP list

The MP list is the preferred service location source for a client, because it is a prioritized list of management points that the client previously identified. This list is sorted by each client based on its network location when the client updates the list, and then stored locally on the client in WMI.

Building the initial MP list

During installation of the client, the following rules are used to build the client's initial MP list:

- The initial list includes management points specified during client installation (when you use the **SMSMP**= or **/MP** option).
- The client queries AD DS for published management points. To be identified from AD DS, the management point must be from the client's assigned site, and it must be of the same product version as the client.
- If no management point was specified during client installation, and the Active Directory schema is not extended, the client checks DNS and WINS for published management points.
- When the client builds the initial list, information about some management points in the hierarchy might not be known.

Organizing the MP list

Clients organize their list of management points by using the following classifications:

- **Proxy**: A management point at a secondary site.
- **Local**: Any management point that is associated with the client's current network location, as defined by site boundaries. Note the following information about boundaries:
  - When a client belongs to more than one boundary group, the list of local management points is determined from the union of all boundaries that include the current network location of the client.
  - Local management points are typically a subset of a client's assigned management points, unless the client is in a network location that is associated with another site with management points servicing its boundary groups.
- **Assigned**: Any management point that is a site system for the client's assigned site.

You can use preferred management points. Management points at a site that are not associated with a boundary group, or that are not in a boundary group associated with a client's current network location, are not considered preferred. They will be used when the client cannot identify an available preferred management point.

Selecting a management point to use

For typical communications, a client attempts to use a use a management point from the classifications in the following order, based on the client's network location:

1. Proxy
2. Local
3. Assigned

However, the client always uses the assigned management point for registration messages and certain policy messages, even when other communications are sent to a proxy or local management point.

Within each classification (proxy, local, or assigned), the client attempts to use a management point based on preferences, in the following order:

1. HTTPS capable in a trusted or local forest (when the client is configured for HTTPS communication)
2. HTTPS capable not in a trusted or local forest (when the client is configured for HTTPS communication)
3. HTTP capable in a trusted or local forest

4. HTTP capable not in a trusted or local forest

From the set of management points sorted by preferences, the client attempts to use the first management point on the list. This sorted list of management points is random and cannot be ordered. The order of the list can change each time the client updates its MP list.

When a client cannot establish contact with the first management point, it tries each successive management point on its list. It tries each preferred management point in the classification before trying the non-preferred management points. If a client cannot successfully communicate with any management point in the classification, it attempts to contact a preferred management point from the next classification, and so on, until it finds a management point to use.

After a client establishes communication with a management point, it continues to use that same management point until:

- 25 hours have passed.
- The client is unable to communicate with the management point for five attempts over a period of 10 minutes.

The client then randomly selects a new management point to use.

Active Directory

Clients that are domain joined can use AD DS for service location. This requires sites to publish data to Active Directory.

A client can use AD DS for service location when all the following conditions are true:

- The Active Directory schema has been extended or was extended for System Center 2012 Configuration Manager.
- The Active Directory forest is configured for publishing, and Configuration Manager sites are configured to publish.
- The client computer is a member of an Active Directory domain and can access a global catalog server.

If a client cannot find a management point to use for service location from AD DS, it attempts to use DNS.

DNS

Clients on the intranet can use DNS for service location. This requires at least one site in a hierarchy to publish information about management points to DNS.

Consider using DNS for service location when any of the following conditions are true:

- The AD DS schema is not extended to support Configuration Manager.
- Clients on the intranet are located in a forest that is not enabled for Configuration Manager publishing.
- You have clients on workgroup computers, and those clients are not configured for internet-only client management. (A workgroup client configured for the internet will communicate only with internet-facing management points and will not use DNS for service location.)
- You can configure clients to find management points from DNS.

When a site publishes service location records for management points to DNS:

- Publishing is applicable only to management points that accept client connections from the intranet.
- Publishing adds a service location resource record (SRV RR) in the DNS zone of the management point computer. There must be a corresponding host entry in DNS for that computer.

By default, domain-joined clients search DNS for management point records from the client's local domain. You can configure a client property that specifies a domain suffix for a domain that has management point information

published to DNS.

For more information about how to configure the DNS suffix client property, see How to configure client computers to find management points by using DNS publishing in System Center Configuration Manager.

If a client cannot find a management point to use for service location from DNS, it attempts to use WINS.

Publish management points to DNS

To publish management points to DNS, the following two conditions must be true:

- Your DNS servers support service location resource records, by using a version of BIND that is at least 8.1.2.
- The specified intranet FQDNs for the management points in Configuration Manager have host entries (for example, A records) in DNS.

> **IMPORTANT**
> Configuration Manager DNS publishing does not support a disjoint namespace. If you have a disjoint namespace, you can manually publish management points to DNS or use one of the other service location methods that are documented in this section.

When your DNS servers support automatic updates, you can configure Configuration Manager to automatically publish management points on the intranet to DNS, or you can manually publish these records to DNS. When management points are published to DNS, their intranet FQDN and port number are published in the service location (SRV) record. You configure DNS publishing at a site in the site's Management Point Component Properties. For more information, see Site components for System Center Configuration Manager.

When your DNS zone is set to "Secure only" for dynamic updates, only the first management point to publish to DNS can do so successfully with default permissions.

If only one management point can successfully publish and change its DNS record, and the management point server is healthy, clients can get the full MP list from that management point and then find their preferred management point.

When your DNS servers do not support automatic updates but do support service location records, you can manually publish management points to DNS. To accomplish this, you must manually specify the service location resource record (SRV RR) in DNS.

Configuration Manager supports RFC 2782 for service location records. These records have the following format:
_Service._Proto.Name TTL Class SRV Priority Weight Port Target

To publish a management point to Configuration Manager, specify the following values:

- **_Service**: Enter **_mssms_mp_**<sitecode>, where <sitecode> is the management point's site code.
- **._Proto**: Specify **._tcp**.
- **.Name**: Enter the DNS suffix of the management point, for example **contoso.com**.
- **TTL**: Enter **14400**, which is four hours.
- **Class**: Specify **IN** (in compliance with RFC 1035).
- **Priority**: Configuration Manager does not use this field.
- **Weight**: Configuration Manager does not use this field.
- **Port**: Enter the port number that the management point uses, for example **80** for HTTP and **443** for HTTPS.

> **NOTE**
> The SRV record port should match the communication port that the management point uses. By default, this is **80** for HTTP communication and **443** for HTTPS communication.

- **Target**: Enter the intranet FQDN that is specified for the site system that is configured with the management point site role.

If you use Windows Server DNS, you can use the following procedure to enter this DNS record for intranet management points. If you use a different implementation for DNS, use the information in this section about the field values and consult that DNS documentation to adapt this procedure.

To configure automatic publishing:

1. In the Configuration Manager console, expand **Administration** > **Site Configuration** > **Sites**.
2. Select your site and then choose **Configure Site Components**.
3. Choose **Management Point**.
4. Select the management points that you want to publish. (This selection applies to publishing to AD DS and DNS.)
5. Check the box to publish to DNS. This box:
   - Lets you select which management points to publish to DNS.
   - Does not configure publishing to AD DS.

To manually publish management points to DNS on Windows Server

1. In the Configuration Manager console, specify the intranet FQDNs of site systems.
2. In the DNS management console, select the DNS zone for the management point computer.
3. Verify that there is a host record (A or AAAA) for the intranet FQDN of the site system. If this record does not exist, create it.
4. By using the **New Other Records** option, choose **Service Location (SRV)** in the **Resource Record Type** dialog box, choose **Create Record**, enter the following information, and then choose **Done**:
   - **Domain**: If necessary, enter the DNS suffix of the management point, for example **contoso.com**.
   - **Service**: Type **_mssms_mp_**<sitecode>, where <sitecode> is the management point's site code.
   - **Protocol**: Type **_tcp**.
   - **Priority**: Configuration Manager does not use this field.
   - **Weight**: Configuration Manager does not use this field.
   - **Port**: Enter the port number that the management point uses, for example **80** for HTTP and **443** for HTTPS.

     > **NOTE**
     > The SRV record port should match the communication port that the management point uses. By default, this is **80** for HTTP communication and **443** for HTTPS communication.

   - **Host offering this service**: Enter the intranet FQDN that is specified for the site system that is configured with the management point site role.

Repeat these steps for each management point on the intranet that you want to publish to DNS.

WINS

When other service location mechanisms fail, clients can find an initial management point by checking WINS.

By default, a primary site publishes to WINS the first management point at the site that is configured for HTTP and the first management point that is configured for HTTPS.

If you do not want clients to find an HTTP management point in WINS, configure clients with the CCMSetup.exe Client.msi property **SMSDIRECTORYLOOKUP=NOWINS**.

Security and privacy for site administration in Configuration Manager

7/26/2019 • 20 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article contains security and privacy information for Configuration Manager sites and the hierarchy.

Security guidance for site administration

Use the following guidance to help you secure Configuration Manager sites and the hierarchy.

Run setup from a trusted source and secure communication

To help prevent someone from tampering with the source files, run Configuration Manager setup from a trusted source. If you store the files on the network, secure the network location.

If you do run setup from a network location, to help prevent an attacker from tampering with the files as they're transmitted over the network, use IPsec or SMB signing between the source location of the setup files and the site server.

If you use the Setup Downloader to download the files that are required by setup, make sure that you secure the location where these files are stored. Also secure the communication channel for this location when you run setup.

Extend the Active Directory schema and publish sites to the domain

Schema extensions aren't required to run Configuration Manager, but they do create a more secure environment. Clients and site servers can retrieve information from a trusted source.

If clients are in an untrusted domain, deploy the following site system roles in the clients' domains:

- Management point
- Distribution point

> **NOTE**
> A trusted domain for Configuration Manager requires Kerberos authentication. If clients are in another forest that doesn't have a two-way forest trust with the site server's forest, these clients are considered to be in an untrusted domain. An external trust isn't sufficient for this purpose.

Use IPsec to secure communications

Although Configuration Manager does secure communication between the site server and the computer that runs SQL Server, Configuration Manager doesn't secure communications between site system roles and SQL Server. You can only configure some site systems with HTTPS for intrasite communication.

If you don't use additional controls to secure these server-to-server channels, attackers can use various spoofing and man-in-the-middle attacks against site systems. Use SMB signing when you can't use IPsec.

> **IMPORTANT**
> Secure the communication channel between the site server and the package source server. This communication uses SMB. If you can't use IPsec to secure this communication, use SMB signing to make sure that the files aren't tampered with before clients download and run them.

Don't change the default security groups

Don't change the following security groups that Configuration Manager creates and manages for site system communication:

- **SMS_SiteSystemToSiteServerConnection_MP_<SiteCode>**
- **SMS_SiteSystemToSiteServerConnection_SMSProv_<SiteCode>**
- **SMS_SiteSystemToSiteServerConnection_Stat_<SiteCode>**

Configuration Manager automatically creates and manages these security groups. This behavior includes removing computer accounts when a site system role is removed.

To make sure service continuity and least privileges, don't manually edit these groups.

Manage the trusted root key provisioning process

If clients can't query the global catalog for Configuration Manager information, they must rely on the trusted root key to authenticate valid management points. The trusted root key is stored in the client registry. It can be set by using group policy or manual configuration.

If the client doesn't have a copy of the trusted root key before it contacts a management point for the first time, it trusts the first management point it communicates with. To reduce the risk of an attacker misdirecting clients to an unauthorized management point, you can pre-provision the clients with the trusted root key. For more information, see Planning for the trusted root key.

Use non-default port numbers

Using non-default port numbers can provide additional security. They make it harder for attackers to explore the environment in preparation for an attack. If you decide to use non-default ports, plan for them before you install Configuration Manager. Use them consistently across all sites in the hierarchy. Client request ports and Wake On LAN are examples where you can use non-default port numbers.

Use role separation on site systems

Although you can install all the site system roles on a single computer, this practice is rarely used on production networks. It creates a single point of failure.

Reduce the attack profile

Isolating each site system role on a different server reduces the chance that an attack against vulnerabilities on one site system can be used against a different site system. Many roles require the installation of Internet Information Services (IIS) on the site system, and this need increases the attack surface. If you must combine roles to reduce hardware expenditure, combine IIS roles only with other roles that require IIS.

> **IMPORTANT**
> The fallback status point role is an exception. Because this site system role accepts unauthenticated data from clients, don't assign the fallback status point role to any other Configuration Manager site system role.

Configure static IP addresses for site systems

Static IP addresses are easier to protect from name resolution attacks.

Static IP addresses also make the configuration of IPsec easier. Using IPsec is a security best practice for securing communication between site systems in Configuration Manager.

Don't install other applications on site system servers

When you install other applications on site system servers, you increase the attack surface for Configuration Manager. You also risk incompatibility issues.

Require signing and enable encryption as a site option

Enable the signing and encryption options for the site. Ensure that all clients can support the SHA-256 hash algorithm, and then enable the option to **Require SHA-256**.

Restrict and monitor administrative users

Grant administrative access to Configuration Manager only to users that you trust. Then grant them minimum permissions by using the built-in security roles or by customizing the security roles. Administrative users who can create, modify, and deploy software and configurations can potentially control devices in the Configuration Manager hierarchy.

Periodically audit administrative user assignments and their authorization level to verify required changes.

For more information, see Configure role-based administration.

Secure Configuration Manager backups

When you back up Configuration Manager, this information includes certificates and other sensitive data that could be used by an attacker for impersonation.

Use SMB signing or IPsec when you transfer this data over the network, and secure the backup location.

Secure locations for exported objects

Whenever you export or import objects from the Configuration Manager console to a network location, secure the location and secure the network channel.

Restrict who can access the network folder.

To prevent an attacker from tampering with the exported data, use SMB signing or IPsec between the network location and the site server. Also secure the communication between the computer that runs the Configuration Manager console and site server. Use IPsec to encrypt the data on the network to prevent information disclosure.

Manually remove certificates from failed servers

If a site system isn't uninstalled properly, or stops functioning and can't be restored, manually remove the Configuration Manager certificates for this server from other Configuration Manager servers.

To remove the peer trust that was originally established with the site system and site system roles, manually remove the Configuration Manager certificates for the failed server in the **Trusted People** certificate store on other site system servers. This action is important if you reuse the server without reformatting it.

For more information, see Cryptographic controls for server communication.

Don't configure internet-based site systems to bridge the perimeter network

Don't configure site system servers to be multi-homed so that they connect to the perimeter network and the intranet. Although this configuration allows internet-based site systems to accept client connections from the internet and the intranet, it eliminates a security boundary between the perimeter network and the intranet.

Configure the site server to initiate connections to perimeter networks

If a site system is on an untrusted network, such as a perimeter network, configure the site server to initiate connections to the site system.

By default, site systems initiate connections to the site server to transfer data. This configuration can be a security

risk when the connection initiation is from an untrusted network to the trusted network. When site systems accept connections from the internet, or reside in an untrusted forest, configure the site system option to **Require the site server to initiate connections to this site system**. After the installation of the site system and any roles, all connections are initiated by the site server from the trusted network.

Use SSL bridging and termination with authentication

If you use a web proxy server for internet-based client management, use SSL bridging to SSL, by using termination with authentication.

When you configure SSL termination at the proxy web server, packets from the internet are subject to inspection before they're forwarded to the internal network. The proxy web server authenticates the connection from the client, terminates it, and then opens a new authenticated connection to the internet-based site systems.

When Configuration Manager client computers use a proxy web server to connect to internet-based site systems, the client identity (GUID) is securely contained within the packet payload. Then the management point doesn't consider the proxy web server to be the client.

If your proxy web server can't support the requirements for SSL bridging, SSL tunneling is also supported. This option is less secure. The SSL packets from the internet are forwarded to the site systems without termination. Then they can't be inspected for malicious content.

> **WARNING**
> Mobile devices that are enrolled by Configuration Manager can't use SSL bridging. They must use SSL tunneling only.

Configurations to use if you configure the site to wake up computers to install software

- If you use traditional wake-up packets, use unicast rather than subnet-directed broadcasts.
- If you must use subnet-directed broadcasts, configure routers to allow IP-directed broadcasts only from the site server and only on a non-default port number.

For more information about the different Wake On LAN technologies, see Planning how to wake up clients.

If you use email notification, configure authenticated access to the SMTP mail server

Whenever possible, use a mail server that supports authenticated access. Use the computer account of the site server for authentication. If you must specify a user account for authentication, use an account that has the least privileges.

Security guidance for the site server

Use the following guidance to help you secure the Configuration Manager site server.

Install Configuration Manager on a member server instead of a domain controller

The Configuration Manager site server and site systems don't require installation on a domain controller. Domain controllers don't have a local Security Accounts Management (SAM) database other than the domain database. When you install Configuration Manager on a member server, you can maintain Configuration Manager accounts in the local SAM database rather than in the domain database.

This practice also lowers the attack surface on your domain controllers.

Install secondary sites without copying the files over the network

When you run setup and create a secondary site, don't select the option to copy the files from the parent site to the secondary site. Also don't use a network source location. When you copy files over the network, a skilled attacker could hijack the secondary site installation package and tamper with the files before they're installed. Timing this attack would be difficult. This attack can be mitigated by using IPsec or SMB when you transfer the files.

Instead of copying the files over the network, on the secondary site server, copy the source files from media folder to a local folder. Then, when you run setup to create a secondary site, on the **Installation Source Files** page, select **Use the source files at the following location on the secondary site computer (most secure)**, and specify this folder.

For more information, see Install a secondary site.

Site role installation inherits permissions from drive root

Make sure to properly configure the system drive permissions before you install the first site system role to any server. For example, `C:\SMS_CCM` inherits permissions from `C:\`. If the root of the drive isn't properly secured, then low rights users may be able to access or modify content in the Configuration Manager folder.

Security guidance for SQL Server

Configuration Manager uses SQL Server as the back-end database. If the database is compromised, attackers could bypass Configuration Manager. If they access SQL Server directly, they can launch attacks through Configuration Manager. Consider attacks against SQL Server to be high risk and mitigate appropriately.

Use the following security guidance to help you secure SQL Server for Configuration Manager.

Don't use the Configuration Manager site database server to run other SQL Server applications

When you increase the access to the Configuration Manager site database server, this action increases the risk to your Configuration Manager data. If the Configuration Manager site database is compromised, other applications on the same SQL Server computer are then also put at risk.

Configure SQL Server to use Windows authentication

Although Configuration Manager accesses the site database by using a Windows account and Windows authentication, it's still possible to configure SQL Server to use SQL Server mixed mode. SQL Server mixed mode allows additional SQL sign-ins to access the database. This configuration isn't required and increases the attack surface.

Update SQL Server Express at secondary sites

When you install a primary site, Configuration Manager downloads SQL Server Express from the Microsoft Download Center. It then copies the files to the primary site server. When you install a secondary site and select the option that installs SQL Server Express, Configuration Manager installs the previously downloaded version. It doesn't check whether new versions are available. To make sure that the secondary site has the latest versions, do one of the following tasks:

- After you install the secondary site, run Windows Update on the secondary site server.
- Before you install the secondary site, manually install SQL Server Express on the secondary site server. Make sure that you install the latest version and any software updates. Then install the secondary site, and select the option to use an existing SQL Server instance.

Periodically run Windows Update for all installed versions of SQL Server. This practice makes sure that they have the latest software updates.

Follow general guidance for SQL Server

Identify and follow the general guidance for your version of SQL Server. However, take into consideration the following requirements for Configuration Manager:

- The computer account of the site server must be a member of the Administrators group on the computer that runs SQL Server. If you follow the SQL Server recommendation of "provision administrator principals explicitly", the account that you use to run setup on the site server must be a member of the SQL Users group.

- If you install SQL Server by using a domain user account, make sure that the site server computer account is configured for a Service Principal Name (SPN) that's published to Active Directory Domain Services. Without the SPN, Kerberos authentication fails and Configuration Manager setup fails.

Security guidance for site systems that run IIS

Several site system roles in Configuration Manager require IIS. The process of securing IIS enables Configuration Manager to operate correctly and reduces the risk of security attacks. When practical, minimize the number of servers that require IIS. For example, run only the number of management points that you require to support your client base, taking into consideration high availability and network isolation for internet-based client management.

Use the following guidance to help you secure the site systems that run IIS.

Disable IIS functions that you don't require

Install only the minimum IIS features for the site system role that you install. For more information, see Site and site system prerequisites.

Configure the site system roles to require HTTPS

When clients connect to a site system by using HTTP rather than by using HTTPS, they use Windows authentication. This behavior might fall back to using NTLM authentication rather than Kerberos authentication. When NTLM authentication is used, clients might connect to a rogue server.

The exception to this guidance might be distribution points. Package access accounts don't work when the distribution point is configured for HTTPS. Package access accounts provide authorization to the content, so that you can restrict which users can access the content. For more information, see Security best practices for content management.

Configure a certificate trust list (CTL) in IIS for site system roles

Site system roles:

- A distribution point that you configure for HTTPS
- A management point that you configure for HTTPS and enable to support mobile devices

A CTL is a defined list of trusted root certification authorities (CAs). When you use a CTL with group policy and a public key infrastructure (PKI) deployment, a CTL enables you to supplement the existing trusted root CAs that are configured on your network. For example, CAs that are automatically installed with Microsoft Windows or added through Windows enterprise root CAs. When a CTL is configured in IIS, it defines a subset of those trusted root CAs.

This subset provides you with more control over security. The CTL restricts the client certificates that are accepted to only those certificates that are issued from the list of CAs in the CTL. For example, Windows comes with a number of well-known, third-party CA certificates, such as VeriSign and Thawte.

By default, the computer that runs IIS trusts certificates that chain to these well-known CAs. When you don't configure IIS with a CTL for the listed site system roles, the site accepts as a valid client any device that has a certificate issued from these CAs. If you configure IIS with a CTL that didn't include these CAs, the site refuses client connections, if the certificate chains to these CAs. For Configuration Manager clients to be accepted for the listed site system roles, you must configure IIS with a CTL that specifies the CAs that are used by Configuration Manager clients.

> **NOTE**
> Only the listed site system roles require you to configure a CTL in IIS. The certificate issuers list that Configuration Manager uses for management points provides the same functionality for client computers when they connect to HTTPS management points.

For more information about how to configure a list of trusted CAs in IIS, see the IIS documentation.

Don't put the site server on a computer with IIS

Role separation helps to reduce the attack profile and improve recoverability. The computer account of the site server typically has administrative privileges on all site system roles. It may also have these privileges on Configuration Manager clients, if you use client push installation.

Use dedicated IIS servers for Configuration Manager

Although you can host multiple web-based applications on the IIS servers that are also used by Configuration Manager, this practice can significantly increase your attack surface. A poorly configured application could allow an attacker to gain control of a Configuration Manager site system. This breach could allow an attacker to gain control of the hierarchy.

If you must run other web-based applications on Configuration Manager site systems, create a custom web site for Configuration Manager site systems.

Use a custom website

For site systems that run IIS, configure Configuration Manager to use a custom website instead of the default website. If you have to run other web applications on the site system, you must use a custom website. This setting is a site-wide setting rather than a setting for a specific site system.

When you use custom websites, remove the default virtual directories

When you change from using the default website to using a custom website, Configuration Manager doesn't remove the old virtual directories. Remove the virtual directories that Configuration Manager originally created under the default website.

For example, remove the following virtual directories for a distribution point:

- SMS_DP_SMSPKG$
- SMS_DP_SMSSIG$
- NOCERT_SMS_DP_SMSPKG$
- NOCERT_SMS_DP_SMSSIG$

Follow IIS Server security guidance

Identify and follow the general guidance for your version of IIS Server. Take into consideration any requirements that Configuration Manager has for specific site system roles. For more information, see Site and site system prerequisites.

Security guidance for the management point

Management points are the primary interface between devices and Configuration Manager. Consider attacks against the management point and the server that it runs on to be high risk, and mitigate appropriately. Apply all appropriate security guidance and monitor for unusual activity.

Use the following guidance to help secure a management point in Configuration Manager.

Assign the client on a management point to the same site

Avoid the scenario where you assign the Configuration Manager client that's on a management point to a site other than the management point's site.

If you migrate from an earlier version to Configuration Manager current branch, migrate the client on the management point to the new site as soon as possible.

Security guidance for the fallback status point

If you install a fallback status point in Configuration Manager, use the following security guidance:

For more information about the security considerations when you install a fallback status point, see Determine whether you require a fallback status point.

Don't run any other roles on the same site system

The fallback status point is designed to accept unauthenticated communication from any computer. If you run this site system role with other roles or a domain controller, the risk to that server greatly increases.

Install the fallback status point before you install clients with PKI certificates

If Configuration Manager site systems don't accept HTTP client communication, you might not know that clients are unmanaged because of PKI-related certificate issues. If you assign clients to a fallback status point, they report these certificate issues through the fallback status point.

For security reasons, you can't assign a fallback status point to clients after they're installed. You can only assign this role during client installation.

Avoid using the fallback status point in the perimeter network

By design, the fallback status point accepts data from any client. Although a fallback status point in the perimeter network could help you to troubleshoot internet-based clients, balance the troubleshooting benefits with the risk of a site system that accepts unauthenticated data in a publicly accessible network.

If you do install the fallback status point in the perimeter network or any untrusted network, configure the site server to initiate data transfers. Don't use the default setting that allows the fallback status point to initiate a connection to the site server.

Security issues for site administration

Review the following security issues for Configuration Manager:

- Configuration Manager has no defense against an authorized administrative user who uses Configuration Manager to attack the network. Unauthorized administrative users are a high security risk. They could launch many attacks, which include the following strategies:
  - Use software deployment to automatically install and run malicious software on every Configuration Manager client computer in the organization.
  - Remotely control a Configuration Manager client without client permission.
  - Configure rapid polling intervals and extreme amounts of inventory. This action creates denial of service attacks against the clients and servers.
  - Use one site in the hierarchy to write data to another site's Active Directory data.

  The site hierarchy is the security boundary. Consider sites to be management boundaries only.

  Audit all administrative user activity and routinely review the audit logs. Require all Configuration Manager administrative users to undergo a background check before they're hired. Require periodic rechecks as a condition of employment.

- If the enrollment point is compromised, an attacker could obtain certificates for authentication. They could steal the credentials of users who enroll their mobile devices.

  The enrollment point communicates with a CA. It can create, modify, and delete Active Directory objects. Never install the enrollment point in the perimeter network. Always monitor for unusual activity.

- If you allow user policies for internet-based client management, you increase your attack profile.

  In addition to using PKI certificates for client-to-server connections, these configurations require Windows authentication. They might fall back to using NTLM authentication rather than Kerberos. NTLM authentication is vulnerable to impersonation and replay attacks. To successfully authenticate a user on the internet, you need to allow a connection from the internet-based site system to a domain controller.

- The **Admin$** share is required on site system servers.

  The Configuration Manager site server uses the Admin$ share to connect to and do service operations on site systems. Don't disable or remove this share.

- Configuration Manager uses name resolution services to connect to other computers. These services are hard to secure against the following security attacks:

  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial of service
  - Elevation of privilege

  Identify and follow any security guidance for the version of DNS that you use for name resolution.

Privacy information for discovery

Discovery creates records for network resources and stores them in the Configuration Manager database. Discovery data records contain computer information such as IP addresses, OS versions, and computer names. You can also configure Active Directory discovery methods to return any information that your organization stores in Active Directory Domain Services.

The only discovery method that Configuration Manager enables by default is Heartbeat Discovery. This method only discovers computers that already have the Configuration Manager client software installed.

Discovery information isn't directly sent to Microsoft. It's stored in the Configuration Manager database. Configuration Manager retains information in the database until it deletes the data. This process happens every 90 days by the site maintenance task **Delete Aged Discovery Data**.

Network infrastructure considerations for Configuration Manager

6/20/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To prepare your network to support Configuration Manager, you may need to configure some infrastructure components. For example, open firewall ports to pass the communications used by Configuration Manager.

Ports and protocols

Different Configuration Manager features use different network ports. Some ports are required, and some you can customize.

Most Configuration Manager communications use common ports like port 80 for HTTP or 443 for HTTPS. Some site system roles support the use of custom websites and custom ports. For more information, see Websites for site system servers.

Before you deploy Configuration Manager, identify the ports that you plan to use, and set up firewalls as needed.

After you install Configuration Manager, if you need to change a port, don't forget to update firewalls on devices and the network. Also change the configuration of the port in Configuration Manager.

For more information, see the following articles:

- How to configure client communication ports
- Ports used in Configuration Manager

Internet access requirements

Some Configuration Manager features rely on internet connectivity for full functionality. If your organization restricts network communication with the internet using a firewall or proxy device, make sure to allow the necessary endpoints.

For more information, see Internet access requirements

Proxy servers

You can specify separate proxy servers for different site system servers and clients. You make these configurations when you install a site system role or client, or change them later as needed.

For more information, see Proxy server support.

Ports used in Configuration Manager

7/19/2019 • 20 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article lists the network ports that Configuration Manager uses. Some connections use ports that aren't configurable, and some support custom ports that you specify. If you use any port filtering technology, verify that the required ports are available. These port filtering technologies include firewalls, routers, proxy servers, or IPsec.

> **NOTE**
> If you support internet-based clients by using SSL bridging, in addition to port requirements, you might also have to allow some HTTP verbs and headers to traverse your firewall.

Ports you can configure

Configuration Manager enables you to configure the ports for the following types of communication:

- Application Catalog website point to Application Catalog web service point
- Enrollment proxy point to enrollment point
- Client-to-site systems that run IIS
- Client to internet (as proxy server settings)
- Software update point to internet (as proxy server settings)
- Software update point to WSUS server
- Site server to site database server
- Reporting services points

  > **NOTE**
  > The ports that are in use for the reporting services point site system role are configured in SQL Server Reporting Services. These ports are then used by Configuration Manager during communications to the reporting services point. Be sure to review these ports that define the IP filter information for IPsec policies or for configuring firewalls.

By default, the HTTP port that's used for client-to-site system communication is port 80, and the default HTTPS port is 443. Ports for client-to-site system communication over HTTP or HTTPS can be changed during setup or in the site properties for your Configuration Manager site.

The ports that are in use for the reporting services point site system role are configured in SQL Server Reporting Services. These ports are then used by Configuration Manager during communications to the reporting services point. Be sure to review these ports when you're defining the IP filter information for IPsec policies or for configuring firewalls.

Non-configurable ports

Configuration Manager doesn't allow you to configure ports for the following types of communication:

- Site to site
- Site server to site system
- Configuration Manager console to SMS Provider
- Configuration Manager console to the internet
- Connections to cloud services, such as Microsoft Intune and cloud distribution points

Ports used by Configuration Manager clients and site systems

The following sections detail the ports that are used for communication in Configuration Manager. The arrows in the section title show the direction of the communication:

- -- > Indicates that one computer initiates communication and the other computer always responds
- < -- > Indicates that either computer can initiate communication

Asset Intelligence synchronization point -- > Microsoft

DESCRIPTION	UDP	TCP
HTTPS	--	443

Asset Intelligence synchronization point -- > SQL Server

DESCRIPTION	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Application Catalog web service point -- > SQL Server

DESCRIPTION	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Application Catalog website point -- > Application Catalog web service point

DESCRIPTION	UDP	TCP
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available

Client -- > Application Catalog website point

DESCRIPTION	UDP	TCP
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available

Client -- > Client

In addition to the ports that are listed in this table, wake-up proxy also uses ICMP echo request messages from one client to another client. Clients use this communication to confirm whether the other client is awake on the network. ICMP is sometimes referred to as ping commands. ICMP doesn't have a UDP or TCP protocol number,

and so it isn't listed in the below table. However, any host-based firewalls on these client computers or intervening network devices within the subnet must permit ICMP traffic for wake-up proxy communication to succeed.

DESCRIPTION	UDP	TCP
Wake On LAN	9 Note 2 Alternate port available	--
Wake-up proxy	25536 Note 2 Alternate port available	--
Windows PE Peer cache broadcast	8004	--
Windows PE Peer cache download	--	8003

For more information, see Windows PE Peer Cache.

Client -- > Configuration Manager Network Device Enrollment Service (NDES) policy module

DESCRIPTION	UDP	TCP
HTTP		80
HTTPS	--	443

Client -- > Cloud distribution point

DESCRIPTION	UDP	TCP
HTTPS	--	443

For more information, see Ports and data flow.

Client -- > Cloud management gateway (CMG)

DESCRIPTION	UDP	TCP
HTTPS	--	443

For more information, see CMG Ports and data flow.

Client -- > Distribution point

DESCRIPTION	UDP	TCP
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available

Client -- > Distribution point configured for multicast

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
Multicast protocol	63000-64000	--

Client -- > Distribution point configured for PXE

DESCRIPTION	UDP	TCP
DHCP	67 and 68	--
TFTP	69 Note 4	--
Boot Information Negotiation Layer (BINL)	4011	--

> **IMPORTANT**
> If you enable a host-based firewall, make sure that the rules allow the server to send and receive on these ports. When you enable a distribution point for PXE, Configuration Manager can enable the inbound (receive) rules on the Windows Firewall. It doesn't configure the outbound (send) rules.

Client -- > Fallback status point

DESCRIPTION	UDP	TCP
HTTP	--	80 Note 2 Alternate port available

Client -- > Global catalog domain controller

A Configuration Manager client doesn't contact a global catalog server when it's a workgroup computer or when it's configured for internet-only communication.

DESCRIPTION	UDP	TCP
Global catalog LDAP	--	3268

Client -- > Management point

DESCRIPTION	UDP	TCP
Client notification (default communication before falling back to HTTP or HTTPS)	--	10123 Note 2 Alternate port available
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available

Client -- > Software update point

DESCRIPTION	UDP	TCP
HTTP	--	80 or 8530 Note 3
HTTPS	--	443 or 8531 Note 3

Client -- > State migration point

DESCRIPTION	UDP	TCP
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available
Server Message Block (SMB)	--	445

CMG connection point -- > CMG cloud service

Configuration Manager uses these connections to build the CMG channel. For more information, see CMG Ports and data flow.

DESCRIPTION	UDP	TCP
TCP-TLS (preferred)	--	10140-10155
HTTPS (fallback with one VM)	--	443
HTTPS (fallback with two or more VMs)	--	10124-10139

CMG connection point -- > Management point

Version 1706 or 1710

The specific port depends upon the management point configuration.

DESCRIPTION	UDP	TCP
HTTPS	--	443
HTTP	--	80

Version 1802

DESCRIPTION	UDP	TCP
HTTPS	--	443

For more information, see CMG Ports and data flow.

CMG connection point -- > Software update point

The specific port depends upon the software update point configuration.

DESCRIPTION	UDP	TCP
HTTPS	--	443
HTTP	--	80

For more information, see CMG Ports and data flow.

Configuration Manager console -- > Client

DESCRIPTION	UDP	TCP
Remote Control (control)	--	2701
Remote Assistance (RDP and RTC)	--	3389

Configuration Manager console -- > Internet

DESCRIPTION	UDP	TCP
HTTP	--	80
HTTPS	--	443

The Configuration Manager console uses internet access for the following actions:

- Downloading software updates from Microsoft Update for deployment packages.
- The Feedback item in the ribbon.
- Links to documentation within the console.

Configuration Manager console -- > Reporting services point

DESCRIPTION	UDP	TCP
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available

Configuration Manager console -- > Site server

DESCRIPTION	UDP	TCP
RPC (initial connection to WMI to locate provider system)	--	135

Configuration Manager console -- > SMS Provider

DESCRIPTION	UDP	TCP
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Configuration Manager Network Device Enrollment Service (NDES) policy module -- > Certificate registration point

DESCRIPTION	UDP	TCP
HTTPS	--	443 Note 2 Alternate port available

Data warehouse service point -- > SQL Server

DESCRIPTION	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Distribution point -- > Management point

A distribution point communicates to the management point in the following scenarios:

- To report the status of prestaged content
- To report usage summary data
- To report content validation
- To report the status of package downloads (pull-distribution point)

DESCRIPTION	UDP	TCP
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available

Endpoint Protection point -- > Internet

DESCRIPTION	UDP	TCP
HTTP	--	80

Endpoint Protection point -- > SQL Server

DESCRIPTION	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Enrollment proxy point -- > Enrollment point

DESCRIPTION	UDP	TCP
HTTPS	--	443 Note 2 Alternate port available

Enrollment point -- > SQL Server

DESCRIPTION	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Exchange Server Connector -- > Exchange Online

DESCRIPTION	UDP	TCP
Windows Remote Management over HTTPS	--	5986

Exchange Server Connector -- > On-Premises Exchange Server

DESCRIPTION	UDP	TCP
Windows Remote Management over HTTP	--	5985

Mac computer -- > Enrollment proxy point

DESCRIPTION	UDP	TCP
HTTPS	--	443

Management point -- > Domain controller

DESCRIPTION	UDP	TCP
Lightweight Directory Access Protocol (LDAP)	389	389
Global catalog LDAP	--	3268
RPC Endpoint Mapper	--	135
RPC	--	DYNAMIC Note 6

Management point < -- > Site server

Note 5

DESCRIPTION	UDP	TCP
RPC Endpoint mapper	--	135
RPC	--	DYNAMIC Note 6
Server Message Block (SMB)	--	445

Management point -- > SQL Server

DESCRIPTION	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Mobile device -- > Enrollment proxy point

DESCRIPTION	UDP	TCP
HTTPS	--	443

Mobile device -- > Microsoft Intune

DESCRIPTION	UDP	TCP
HTTPS	--	443

Reporting Services point -- > SQL Server

DESCRIPTION	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Service connection point -- > Microsoft Intune

DESCRIPTION	UDP	TCP
HTTPS	--	443

For more information, see Internet access requirements for the service connection point.

Service connection point -- > Azure (CMG)

DESCRIPTION	UDP	TCP
HTTPS for CMG service deployment	--	443

For more information, see CMG Ports and data flow.

Site server < -- > Application Catalog web service point

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Application Catalog website point

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Asset Intelligence synchronization point

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server -- > Client

DESCRIPTION	UDP	TCP
Wake On LAN	9 Note 2 Alternate port available	--

Site server -- > Cloud distribution point

DESCRIPTION	UDP	TCP
HTTPS	--	443

For more information, see Ports and data flow.

Site server -- > Distribution point

Note 5

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server -- > Domain controller

DESCRIPTION	UDP	TCP
Lightweight Directory Access Protocol (LDAP)	389	389
Global catalog LDAP	--	3268
RPC Endpoint Mapper	--	135
RPC	--	DYNAMIC Note 6

Site server < -- > Certificate registration point

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Endpoint Protection point

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Enrollment point

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135

DESCRIPTION	UDP	TCP
RPC	--	DYNAMIC Note 6

Site server < -- > Enrollment proxy point

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Fallback status point

Note 5

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server -- > Internet

DESCRIPTION	UDP	TCP
HTTP	--	80 Note 1

Site server < -- > Issuing certification authority (CA)

This communication is used when you deploy certificate profiles by using the certificate registration point. The communication isn't used for every site server in the hierarchy. Instead, it's used only for the site server at the top of the hierarchy.

DESCRIPTION	UDP	TCP
RPC Endpoint Mapper	135	135
RPC (DCOM)	--	DYNAMIC Note 6

Site server -- > Server hosting Remote Content Library Share

Starting in version 1806 you can relocate the Content Library to another storage location to free up hard drive space on your central administration or primary site servers. For more information, see Configure a remote content library for the site server.

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445

Site server < -- > Reporting services point

Note 5

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Site server

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445

Site server -- > SQL Server

DESCRIPTION	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

During the installation of a site that uses a remote SQL Server to host the site database, open the following ports between the site server and the SQL Server:

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server -- > SMS Provider

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Software update point

Note 5

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
HTTP	--	80 or 8530 Note 3
HTTPS	--	443 or 8531 Note 3

Site server < -- > State migration point

Note 5

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135

SMS Provider -- > SQL Server

DESCRIPTION	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Software update point -- > Internet

DESCRIPTION	UDP	TCP
HTTP	--	80 Note 1

Software update point -- > Upstream WSUS server

DESCRIPTION	UDP	TCP
HTTP	--	80 or 8530 Note 3
HTTPS	--	443 or 8531 Note 3

SQL Server --> SQL Server

Intersite database replication requires the SQL Server at one site to communicate directly with the SQL Server at its parent or child site.

DESCRIPTION	UDP	TCP
SQL Server service	--	1433 Note 2 Alternate port available
SQL Server Service Broker	--	4022 Note 2 Alternate port available

> **TIP**
> Configuration Manager doesn't require the SQL Server Browser, which uses port UDP 1434.

State migration point -- > SQL Server

DESCRIPTION	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Notes for ports used by Configuration Manager clients and site systems

Note 1: Proxy server port

This port can't be configured but can be routed through a configured proxy server.

Note 2: Alternate port available

An alternate port can be defined within Configuration Manager for this value. If a custom port has been defined, substitute that custom port when defining the IP filter information for IPsec policies or for configuring firewalls.

Note 3: Windows Server Update Services (WSUS)

WSUS can be installed to use either ports 80/443 or ports 8530/8531 for client communication. When you run WSUS in Windows Server 2012 or Windows Server 2016, WSUS is configured by default to use port 8530 for HTTP and port 8531 for HTTPS.

After installation, you can change the port. You don't have to use the same port number throughout the site hierarchy.

- If the HTTP port is 80, the HTTPS port must be 443.
- If the HTTP port is anything else, the HTTPS port must be 1 or higher, for example, 8530 and 8531.

> **NOTE**
> When you configure the software update point to use HTTPS, the HTTP port must also be open. Unencrypted data, such as the EULA for specific updates, uses the HTTP port.

Note 4: Trivial FTP (TFTP) Daemon

The Trivial FTP (TFTP) Daemon system service doesn't require a user name or password and is an integral part of Windows Deployment Services (WDS). The Trivial FTP Daemon service implements support for the TFTP protocol that's defined by the following RFCs:

- RFC 1350: TFTP
- RFC 2347: Option extension
- RFC 2348: Block size option
- RFC 2349: Time-out interval and transfer size options

TFTP is designed to support diskless boot environments. TFTP Daemons listen on UDP port 69 but respond from a dynamically allocated high port. Therefore, enabling this port allows the TFTP service to receive incoming TFTP requests but doesn't allow the selected server to respond to those requests. You can't enable the selected server to respond to inbound TFTP requests unless the TFTP server is configured to respond from port 69.

The PXE-enabled distribution point and the client in Windows PE select dynamically allocated high ports for TFTP transfers. These ports are defined by Microsoft between 49152 and 65535. For more information, see Service overview and network port requirements for Windows

However, during the actual PXE boot, the network card on the device selects the dynamically allocated high port it uses during the TFTP transfer. The network card on the device isn't bound to the dynamically allocated high ports defined by Microsoft. It's only bound to the ports defined in RFC 1350. This port can be any from 0 to 65535. For information regarding what dynamically allocated high ports the network card uses, contact the device hardware manufacturer.

Note 5: Communication between the site server and site systems

By default, communication between the site server and site systems is bi-directional. The site server initiates communication to configure the site system, and then most site systems connect back to the site server to send status information. Reporting service points and distribution points don't send status information. If you select **Require the site server to initiate connections to this site system** on the site system properties after the site system has been installed, the site system won't initiate communication with the site server. Instead, the site server initiates the communication and uses the site system installation account for authentication to the site system server.

Note 6: Dynamic ports

Dynamic ports use a range of port numbers that's defined by the OS version. These ports are also known as ephemeral ports. For more information about the default port ranges, see Service overview and network port requirements for Windows.

Additional lists of ports

The following sections provide additional information about ports that are used by Configuration Manager.

Client to server shares

Clients use Server Message Block (SMB) whenever they connect to UNC shares. For example:

- Manual client installation that specifies the CCMSetup.exe **/source:** command-line property
- Endpoint Protection clients that download definition files from a UNC path

DESCRIPTION	UDP	TCP
Server Message Block (SMB)	--	445

Connections to Microsoft SQL Server

For communication to the SQL Server database engine and for intersite replication, you can use the default SQL Server port or specify custom ports:

- Intersite communications use:
  - SQL Server Service Broker, which defaults to port TCP 4022.
  - SQL Server service, which defaults to port TCP 1433.
- Intrasite communication between the SQL Server database engine and various Configuration Manager site system roles defaults to port TCP 1433.
- Configuration Manager uses the same ports and protocols to communicate with each SQL Availability Group replica that hosts the site database as if the replica was a standalone SQL Server instance.

When you use Azure and the site database is behind an internal or external load balancer, configure the following components:

- Firewall exceptions on each replica
- Load balancing rules

Configure the following ports:

- SQL over TCP: TCP 1433
- SQL Server Service Broker: TCP 4022
- Server Message Block (SMB): TCP 445
- RPC Endpoint Mapper: TCP 135

> **WARNING**
> Configuration Manager doesn't support dynamic ports. by default, SQL Server named instances use dynamic ports for connections to the database engine. When you use a named instance, manually configure the static port for intrasite communication.

The following site system roles communicate directly with the SQL Server database:

- Application Catalog web service point

- Certificate registration point role
- Enrollment point role
- Management point
- Site server
- Reporting Services point
- SMS Provider
- SQL Server --> SQL Server

When a SQL Server hosts a database from more than one site, each database must use a separate instance of SQL Server. Configure each instance with a unique set of ports.

If you enable a host-based firewall on the SQL server, configure it to allow the correct ports. Also configure network firewalls in between computers that communicate with the SQL server.

For an example of how to configure SQL Server to use a specific port, see Configure a server to listen on a specific TCP port.

Discovery and publishing

Configuration Manager uses the following ports for the discovery and publishing of site information:

- Lightweight Directory Access Protocol (LDAP): 389
- Global catalog LDAP: 3268
- RPC Endpoint Mapper: 135
- RPC: Dynamically allocated high TCP ports
- TCP: 1024: 5000
- TCP: 49152: 65535

External connections made by Configuration Manager

On-premises Configuration Manager clients or site systems can make the following external connections:

- Asset Intelligence synchronization point -- > Microsoft
- Endpoint Protection point -- > Internet
- Client -- > Global catalog domain controller
- Configuration Manager console -- > Internet
- Management point -- > Domain controller
- Site server -- > Domain controller
- Site server < -- > Issuing Certification Authority (CA)
- Software update point -- > Internet
- Software update point -- > Upstream WSUS Server
- Service connection point -- > Microsoft Intune
- Service connection point -- > Azure
- CMG connection point -- > CMG cloud service

Installation requirements for site systems that support internet-based clients

> **NOTE**
> This section only applies to internet-based client management (IBCM). It doesn't apply to the cloud management gateway. For more information, see Manage clients on the internet.

Internet-based management points and distribution points that support internet-based clients, the software update point, and the fallback status point use the following ports for installation and repair:

- Site server --> Site system: RPC endpoint mapper using UDP and TCP port 135.
- Site server --> Site system: RPC dynamic TCP ports
- Site server < --> Site system: Server message blocks (SMB) using TCP port 445

Application and package installations on distribution points require the following RPC ports:

- Site server --> Distribution point: RPC endpoint mapper using UDP and TCP port 135
- Site server --> Distribution point: RPC dynamic TCP ports

Use IPsec to help secure the traffic between the site server and site systems. If you must restrict the dynamic ports that are used with RPC, you can use the Microsoft RPC configuration tool (rpccfg.exe) to configure a limited range of ports for these RPC packets. For more information about the RPC configuration tool, see How to configure RPC to use certain ports and how to help secure those ports by using IPsec.

> **IMPORTANT**
> Before you install these site systems, ensure that the remote registry service is running on the site system server and that you have specified a site system installation account if the site system is in a different Active Directory forest without a trust relationship.

Ports used by Configuration Manager client installation

The ports that Configuration Manager uses during client installation depends on the deployment method.

- For a list of ports for each client deployment method, see Ports used during Configuration Manager client deployment
- For more information about how to configure Windows Firewall on the client for client installation and post-installation communication, see Windows Firewall and port settings for clients

Ports used by migration

The site server that runs migration uses several ports to connect to applicable sites in the source hierarchy. For more information, see Required configurations for migration.

Ports used by Windows Server

The following table lists some of the key ports used by Windows Server.

DESCRIPTION	UDP	TCP
DNS	53	53
DHCP	67 and 68	--
NetBIOS Name Resolution	137	--

DESCRIPTION	UDP	TCP
NetBIOS Datagram Service	138	--
NetBIOS Session Service	--	139
Kerberos authentication	--	88

For more information, see the following articles:

- Service overview and network port requirements for the Windows Server system.
- How to configure a firewall for domains and trusts

Proxy server support in Configuration Manager

5/9/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Some Configuration Manager site system servers require connections to the internet. If your environment requires internet traffic to use a proxy server, configure these site system roles to use the proxy.

- A computer that hosts a site system server supports a single proxy server configuration. All site system roles on that computer share this same proxy configuration. If you need separate proxy servers for different roles or instances of a role, place those roles on separate site system servers.
- When you configure new proxy server settings for a site system server that already has a proxy server configuration, the original configuration is overwritten.
- By default, connections to the proxy use the **System** account of the computer that hosts the site system role.
- If the computer account can't authenticate, the site system server can store user credentials to connect to the proxy server. These credentials are the **site system proxy server account**.

Site system roles that use a proxy

The following site system roles connect to the internet, and if necessary, can use a proxy server:

Asset Intelligence synchronization point

This site system role connects to Microsoft and uses a proxy server configuration on the computer that hosts the Asset Intelligence synchronization point.

Cloud distribution point

The cloud distribution point role runs in Microsoft Azure. You don't configure this site system role to use a proxy. Set the proxy configuration on the primary site server that manages the cloud distribution point.

For this configuration, the primary site server:

- Must be able to connect to Microsoft Azure to set up, monitor, and distribute content to the cloud distribution point.
- By default, uses the computer's **System** account to make the connection. It can also use the site system proxy server account, if necessary.
- Uses Windows web browser APIs.

Exchange Server connector

This site system role connects to an Exchange Server. It uses a proxy server configuration on the computer that hosts the Exchange Server connector.

Service connection point

This site system role connects to the Configuration Manager cloud service to download version updates for Configuration Manager, and connects to Microsoft Intune in a hybrid configuration. It uses a proxy server that's configured on the computer that hosts the service connection point.

Software update point

This site system role uses the proxy when it connects to Microsoft Update to download patches and synchronize information about updates. Like every other site system role, first configure the site system proxy settings. Then configure the following options specific to the software update point:

- **Use a proxy server when synchronizing software updates**
- **Use a proxy server when downloading content by using automatic deployment rules**

> **NOTE**
> While available for use, this setting isn't used by software update points at secondary sites.

These settings are on the **Proxy and Account Settings** tab of the software update point properties.

> **NOTE**
> By default, when the automatic deployment rules run, the **System** account on the site server of the site on which an automatic deployment rule was created is used to connect to the internet and download software updates. Alternatively, configure and use the site system proxy server account.
>
> When this account cannot access the internet, software updates fail to download. The following entry is logged to **ruleengine.log**:
>
> ```
> Failed to download the update from internet. Error = 12007.
> ```

Configure the proxy for a site system server

1. In the Configuration Manager console, go to the **Administration** workspace. Expand **Site Configuration**, and then select the **Servers and Site System Roles** node.
2. Select the site system server that you want to edit. In the details pane, right-click the **Site system** role, and select **Properties**.
3. In Site system Properties, switch to the **Proxy** tab. Configure the following proxy settings:
   - **Use a proxy server when synchronizing information from the internet**: Select this option to enable the site system server to use a proxy server.
   - **Proxy server name**: Specify the hostname or FQDN of the proxy server in your environment.
   - **Port**: Specify the network port on which to communicate with the proxy server. By default, it uses port **80**.
   - **Use credentials to connect to the proxy server**: Many proxy servers require a user to authenticate. By default, the site system server uses its computer account to connect to the proxy server. If necessary, enable this option, click **Set**, and then choose an **Existing Account** or specify a **New Account**. These credentials are the **site system proxy server account**. For more information, see Accounts used in Configuration Manager.
4. Choose **OK** to save the new proxy server configuration.

Internet access requirements

9/4/2019 • 4 minutes to read • Edit Online

Some Configuration Manager features rely on internet connectivity for full functionality. If your organization restricts network communication with the internet using a firewall or proxy device, make sure to allow these endpoints.

Service connection point

These configurations apply to the computer that hosts the service connection point and any firewalls between that computer and the internet. They both must allow communications through outgoing port **TCP 443** for HTTPS and outgoing port **TCP 80** for HTTP to the below internet locations.

The service connection point supports using a web proxy (with or without authentication) to use these locations. For more information, see Proxy server support.

For more information on the service connection point, see About the service connection point.

Other Configuration Manager features may require additional endpoints from the service connection point. For more information, see the other sections in this article.

> **TIP**
> The service connection point uses the Microsoft Intune service when it connects to `go.microsoft.com` or `manage.microsoft.com`. There's a known issue in which the Intune connector experiences connectivity issues if the Baltimore CyberTrust Root Certificate isn't installed, is expired, or is corrupted on the service connection point. For more information, see KB 3187516: Service connection point doesn't download updates.

Updates and servicing

For more information on this function, see Updates and servicing for Configuration Manager.

> **TIP**
> Enable these endpoints for the management insight rule, **Connect the site to the Microsoft cloud for Configuration Manager updates**.

- `*.akamaiedge.net`
- `*.akamaitechnologies.com`
- `*.manage.microsoft.com`
- `go.microsoft.com`
- `*.blob.core.windows.net`
- `download.microsoft.com`
- `download.windowsupdate.com`
- `sccmconnected-a01.cloudapp.net`
- `configmgrbits.azureedge.net`

Microsoft Intune

For more information on this function, see Hybrid MDM with Configuration Manager and Microsoft Intune.

- `*manage.microsoft.com`
- `https://bspmts.mp.microsoft.com/V`
- `https://login.microsoftonline.com/{TenantID}`

Windows 10 servicing

For more information on this function, see Manage Windows as a service.

- `download.microsoft.com`
- `https://go.microsoft.com/fwlink/?LinkID=619849`
- `dl.delivery.mp.microsoft.com`

Azure services

For more information on this function, see Configure Azure services for use with Configuration Manager.

- `management.azure.com`

Co-management

If you enroll Windows 10 devices to Microsoft Intune for co-management, make sure those devices can access the endpoints required by Intune. For more information, see Network endpoints for Microsoft Intune.

Microsoft Store for Business

If you integrate Configuration Manager with the Microsoft Store for Business, make sure the service connection point and targeted devices can access the cloud service. For more information, see Microsoft Store for Business proxy configuration.

Cloud services

This section covers the following features:

- Cloud management gateway (CMG)
- Cloud distribution point (CDP)
- Azure Active Directory (Azure AD) integration
- Azure AD-based discovery

For CMG/CDP service deployment, the **service connection point** needs access to:

- Specific Azure endpoints are different per environment depending upon the configuration. Configuration Manager stores these endpoints in the site database. Query the **AzureEnvironments** table in SQL Server for the list of Azure endpoints.

The **CMG connection point** needs access to the following service endpoints:

- ServiceManagementEndpoint: `https://management.core.windows.net/`
- StorageEndpoint: `blob.core.windows.net` and `table.core.windows.net`

For Azure AD token retrieval by the **Configuration Manager console** and **client**:

- ActiveDirectoryEndpoint `https://login.microsoftonline.com/`

For Azure AD user discovery, the **service connection point** needs access to:

- Version 1810 and earlier: Azure AD Graph endpoint `https://graph.windows.net/`
- Version 1902 and later: Microsoft Graph endpoint `https://graph.microsoft.com/`

The cloud management point (CMG) connection point site system supports using a web proxy. For more information on configuring this role for a proxy, see Proxy server support. The CMG connection point only needs to connect to the CMG service endpoints. It doesn't need access to other Azure endpoints.

For more information on the CMG, see Plan for CMG.

Software updates

Allow the active software update point to access the following endpoints so that WSUS and Automatic Updates can communicate with the Microsoft Update cloud service:

- `http://windowsupdate.microsoft.com`
- `http://*.windowsupdate.microsoft.com`
- `https://*.windowsupdate.microsoft.com`
- `http://*.update.microsoft.com`
- `https://*.update.microsoft.com`
- `http://*.windowsupdate.com`
- `http://download.windowsupdate.com`
- `http://download.microsoft.com`
- `http://*.download.windowsupdate.com`
- `http://test.stats.update.microsoft.com`
- `http://ntservicepack.microsoft.com`

For more information on software updates, see Plan for software updates.

Intranet firewall

You might need to add endpoints to a firewall that's between two site systems in the following cases:

- If child sites have a software update point
- If there's a remote active internet-based software update point at a site

Software update point on the child site

- `http://<FQDN for software update point on child site>`
- `https://<FQDN for software update point on child site>`
- `http://<FQDN for software update point on parent site>`
- `https://<FQDN for software update point on parent site>`

Manage Office 365

If you use Configuration Manager to deploy and update Office 365, allow the following endpoints:

- `officecdn.microsoft.com` to synchronize the software update point for Office 365 client updates

- `config.office.com` to create custom configurations for Office 365 deployments

Configuration Manager console

Computers with the Configuration Manager console require access to the following internet endpoints for specific features:

In-console feedback

- `http://petrol.office.microsoft.com`

For more information on this feature, see Product feedback.

Community workspace, Documentation node

- `https://aka.ms`
- `https://raw.githubusercontent.com`

For more information on this console node, see Using the Configuration Manager console.

Monitoring workspace, Site Hierarchy node

If you use the **Geographical View**, allow access to the following endpoint:

- `http://maps.bing.com`

Desktop Analytics

For more information on the required endpoints for the Desktop Analytics cloud service, see Enable data sharing.

Microsoft public IP addresses

For more information on the Microsoft IP address ranges, see Microsoft Public IP Space. These addresses update regularly. There's no granularity by service, any IP address in these ranges could be used.

See also

- Ports used in Configuration Manager
- Proxy server support in Configuration Manager

Prepare Active Directory for site publishing

9/11/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

When you extend the Active Directory schema for System Center Configuration Manager, you introduce new structures to Active Directory that are used by Configuration Manager sites to publish key information in a secure location where clients can easily access it.

It's a good idea to use Configuration Manager with an extended Active Directory schema when you manage on-premises clients. An extended schema can simplify the process of deploying and setting up clients. An extended schema also lets clients efficiently locate resources like content servers and additional services that the different Configuration Manager site system roles provide.

- If you're not familiar with what extended schema provides for a Configuration Manager deployment, you can read about Schema extensions for System Center Configuration Manager to help you make this decision.
- When you don't use an extended schema, you can set up other methods like DNS and WINS to locate services and site system servers. These methods of service location require additional configurations and are not the preferred method for service location by clients. To learn more, read Understand how clients find site resources and services for System Center Configuration Manager,
- If your Active Directory schema was extended for Configuration Manager 2007 or System Center 2012 Configuration Manager, then you don't need to do more. The schema extensions are unchanged and will already be in place.

Extending the schema is a one-time action for any forest. To extend, and then use the extended Active Directory schema, follow these steps:

Step 1. Extend the schema

To extend the schema for Configuration Manager:

- Use an account that is a member of the Schema Admins security group.
- Be signed in to the schema master domain controller.
- Run the **Extadsch.exe** tool, or use the LDIFDE command-line utility with the **ConfigMgr_ad_schema.ldf** file. Both the tool and file are in the **SMSSETUP\BIN\X64** folder on the Configuration Manager installation media.

Option A: Use Extadsch.exe

1. Run **extadsch.exe** to add the new classes and attributes to the Active Directory schema.

   > **TIP**
   > Run this tool from a command line to view feedback while it runs.

2. Verify that the schema extension was successful by reviewing extadsch.log in the root of the system drive.

Option B: Use the LDIF file

1. Edit the **ConfigMgr_ad_schema.ldf** file to define the Active Directory root domain that you want to

extend:

- Replace all instances of the text, **DC=x**, in the file with the full name of the domain to extend.
- For example, if the full name of the domain to extend is named widgets.microsoft.com, change all instances of DC=x in the file to **DC=widgets, DC=microsoft, DC=com**.

2. Use the LDIFDE command-line utility to import the contents of the **ConfigMgr_ad_schema.ldf** file to Active Directory Domain Services:
   - For example, the following command line imports the schema extensions to Active Directory Domain Services, turns on verbose logging, and creates a log file during the import process: **ldifde -i -f ConfigMgr_ad_schema.ldf -v -j <location to store log file>**.
3. To verify that the schema extension was successful, review a log file created by the command line used in the previous step.

Step 2. Create the System Management container and grant sites permissions to the container

After you extend the schema, you must create a container named **System Management** in Active Directory Domain Services (AD DS):

- You create this container one time in each domain that has a primary or secondary site that will publish data to Active Directory.
- For each container, you grant permissions to the computer account of each primary and secondary site server that will publish data to that domain. Each account needs **Full Control** to the container with the advanced permission, **Apply onto**, equal to **This object and all descendant objects**.

To add the container

1. Use an account that has the **Create All Child Objects** permission on the **System** container in Active Directory Domain Services.
2. Run **ADSI Edit** (adsiedit.msc), and connect to the site server's domain.
3. Create the container:
   - Expand **Domain** <computer fully qualified domain name>, expand <distinguished name>, right-click **CN=System**, choose **New**, and then choose **Object**.
   - In the **Create Object** dialog box, choose **Container**, and then choose **Next**.
   - In the **Value** box, enter **System Management**, and then choose **Next**.
4. Assign permissions:

> **NOTE**
> If you prefer, you can use other tools like the Active Directory Users and Computers administrative tool (dsa.msc) to add permissions to the container.

   - Right-click **CN=System Management**, and then choose **Properties**.
   - Choose the **Security** tab, choose **Add**, and then add the site server computer account with the **Full Control** permission.
   - Choose **Advanced**, choose the site server's computer account, and then choose **Edit**.
   - In the **Apply onto** list, choose **This object and all descendant objects**.

5. Choose **OK** to close the console and save the configuration.

Step 3. Set up sites to publish to Active Directory Domain Services

After the container is set up, permissions are granted, and you have installed a Configuration Manager primary site, you can set up that site to publish data to Active Directory.

For more about publishing, see Publish site data for System Center Configuration Manager.

Schema extensions for System Center Configuration Manager

9/11/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can extend the Active Directory schema to support Configuration Manager. This edits a forest's Active Directory schema to add a new container and several attributes that Configuration Manager sites use to publish key information in Active Directory where clients can securely use it. This information can simplify the deployment and configuration of clients and helps clients locate site resources like servers with deployed content or that provide different services to clients.

- It's a good idea to extend the Active Directory schema, but it's not required.

Before you extend the Active Directory schema, you should be familiar with Active Directory Domain Services and comfortable with modifying the Active Directory schema.

Considerations for extending the Active Directory schema for Configuration Manager

- The Active Directory schema extensions for System Center Configuration Manager are unchanged from those that Configuration Manager 2007 and Configuration Manager 2012 use. If you previously extended the schema for either version, you do not have to extend the schema again.
- Extending the schema is a forest-wide, one-time, irreversible action.
- Only a user who is a member of the Schema Admins Group or who has been delegated sufficient permissions to change the schema can extend the schema.
- Although you can extend the schema before or after you run Configuration Manager Setup, it's a good idea to extend the schema before you start to configure your sites and hierarchy settings. This can simplify many of the later configuration steps.
- After you extend the schema, the Active Directory global catalog is replicated throughout the forest. Therefore, plan to extend the schema when the replication traffic will not adversely affect other network-dependent processes:
    - In Windows 2000 forests, extending the schema causes a full sync of the whole global catalog.
    - Beginning with Windows 2003 forests, only the newly added attributes are replicated.

Devices and clients that do not use the Active Directory schema:

- Mobile devices that are managed by the Exchange Server connector
- The client for Mac computers
- The client for Linux and UNIX servers
- Mobile devices that are enrolled by Configuration Manager
- Mobile devices that are enrolled by Microsoft Intune
- Mobile device legacy clients

- Windows clients that are configured for Internet-only client management
- Windows clients that are detected by Configuration Manager to be on the Internet

Capabilities that benefit from extending the schema

Client computer installation and site assignment - When a Windows computer installs a new client, the client searches Active Directory Domain Services for installation properties.

- **Workarounds:** If you do not extend the schema, use one of the following options to provide configuration details that computers must install:
  - **Use client push installation**. Before you use a client installation method, make sure that all prerequisites are met. For more information, see the 'Installation Method Dependencies' section in Prerequisites for deploying clients to Windows computers.
  - **Install clients manually** and provide client installation properties by using CCMSetup installation command-line properties. This must include the following:
    - Specify a management point or source path from which the computer can download the installation files by using the CCMSetup property **/mp:=<management point name computer name>** or **/source:<path to client source files>** on the CCMSetup command line during client installation.
    - Specify a list of initial management points for the client to use so that it can assign them to the site and then download client policy and site settings. Use the CCMSetup Client.msi property SMSMP to do this.
  - **Publish the management point in DNS or WINS** and configure clients to use this service location method.

Port configuration for client-to-server communication - When a client installs, it is configured with port information stored in Active Directory. If you later change the client-to-server communication port for a site, a client can get this new port setting from Active Directory Domain Services.

- **Workarounds:** If you do not extend the schema, use one of the following options to provide new port configurations to existing clients:
  - **Reinstall clients** by using options that configure the new port.
  - **Deploy a custom script to clients that updates the port information**. If clients cannot communicate with a site because of a port change, you cannot use Configuration Manager to deploy this script. For example, you could use Group Policy.

Content deployment scenarios - When you create content at one site and then deploy that content to another site in the hierarchy, the receiving site must be able to verify the signature of the signed content data. This requires access to the public key of the source site where you create this data. When you extend the Active Directory schema for Configuration Manager, a site's public key is available to all sites in the hierarchy.

- **Workaround:** If you do not extend the schema, use the hierarchy maintenance tool, **preinst.exe**, to exchange the secure key information between sites.

  For example, if you plan to create content at a primary site and deploy that content to a secondary site below a different primary site, you must either extend the Active Directory schema to let the secondary site get the source primary site's public key, or use preinst.exe to share keys between the two sites directly.

Active Directory attributes and classes

When you extend the schema for System Center Configuration Manager, the following classes and attributes are added to the schema and available to all Configuration Manager sites in that Active Directory forest.

- Attributes:
  - cn=mS-SMS-Assignment-Site-Code
  - cn=mS-SMS-Capabilities
  - cn=MS-SMS-Default-MP
  - cn=mS-SMS-Device-Management-Point
  - cn=mS-SMS-Health-State
  - cn=MS-SMS-MP-Address
  - cn=MS-SMS-MP-Name
  - cn=MS-SMS-Ranged-IP-High
  - cn=MS-SMS-Ranged-IP-Low
  - cn=MS-SMS-Roaming-Boundaries
    on
  - cn=MS-SMS-Site-Boundaries
  - cn=MS-SMS-Site-Code
  - cn=mS-SMS-Source-Forest
  - cn=mS-SMS-Version
- Classes:
  - cn=MS-SMS-Management-Point
  - cn=MS-SMS-Roaming-Boundary-Range
  - cn=MS-SMS-Server-Locator-Point
  - cn=MS-SMS-Site

> **NOTE**
> The schema extensions might include attributes and classes that are carried forward from previous versions of the product but not used by System Center Configuration Manager. For example:
>
> - Attribute: cn=MS-SMS-Site-Boundaries
>   - Class: cn=MS-SMS-Server-Locator-Point

You can ensure the preceding lists are current by viewing the **ConfigMgr_ad_schema.LDF** file from the **\SMSSETUP\BIN\x64** folder of the System Center Configuration Manager installation media.

Prepare Windows Servers to support Configuration Manager

9/11/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Before you can use a Windows computer as a site system server for Configuration Manager, the computer must meet the prerequisites for its intended use as a site server or site system server.

- These prerequisites often include one or more Windows features or roles, which are enabled by using the computers Server Manager.
- Because the method to enable Windows features and roles differs among OS versions, refer to the documentation for your OS version for detailed information about how to set up the OS that you use.

The information in this article provides an overview of the types of Windows configurations that are required to support Configuration Manager site systems. For configuration details for specific site system roles, see Site and site system prerequisites.

Windows features and roles

When you set up Windows features and roles on a computer, you might be required to reboot the computer to complete that configuration. Therefore, it's a good idea to identify computers that will host specific site system roles before you install a Configuration Manager site or site system server.

Features

The following Windows features are required on certain site system servers and should be set up before you install a site system role on that computer.

- **.NET Framework**: Including
  - ASP.NET
  - HTTP Activation
  - Non-HTTP Activation
  - Windows Communication Foundation (WCF) Services

  Different site system roles require different versions of .NET Framework.

  Because .NET Framework 4.0 and later isn't backward compatible to replace 3.5 and earlier versions, when different versions are listed as required, plan to enable each version on the same computer.
- **Background Intelligent Transfer Services (BITS)**: Management points require BITS (and automatically selected options) to support communication with managed devices.
- **BranchCache**: Distribution points can be set up with BranchCache to support clients that use BranchCache.
- **Data Deduplication**: Distribution points can be set up with and benefit from data deduplication.
- **Remote Differential Compression (RDC)**: Each computer that hosts a site server or a distribution point requires RDC. RDC is used to generate package signatures and perform signature comparisons.

Roles

The following Windows roles are required to support specific functionality, like software updates and OS deployments, while IIS is required by the most common site system roles.

- **Network Device Enrollment Service** (under Active Directory Certificate Services): This Windows role is a prerequisite to use certificate profiles in Configuration Manager.
- **Web server (IIS)**: Including:
  - Common HTTP Features
    - HTTP Redirection
  - Application Development
    - .NET Extensibility
    - ASP.NET
    - ISAPI Extensions
    - ISAPI Filters
  - Management Tools
    - IIS 6 Management Compatibility
    - IIS 6 Metabase Compatibility
    - IIS 6 Windows Management Instrumentation (WMI) Compatibility
  - Security
    - Request Filtering
    - Windows Authentication

  The following site system roles use one or more of the listed IIS configurations:

  - Application Catalog web service point
  - Application Catalog website point
  - Distribution point
  - Enrollment point
  - Enrollment proxy point
  - Fallback status point
  - Management point
  - Software update point
  - State migration point

  The minimum version of IIS that's required is the version that's supplied with the OS of the site server.

  In addition to these IIS configurations, you might need to set up IIS Request Filtering for distribution points.
- **Windows Deployment Services**: This role is used with OS deployment.
- **Windows Server Update Services**: This role is required for software updates.

IIS request filtering for distribution points

By default, IIS uses request filtering to block several file name extensions and folder locations from access by HTTP or HTTPS communication. On a distribution point, this prevents clients from downloading packages that have blocked extensions or folder locations.

When your package source files have extensions that are blocked in IIS by your request filtering configuration, you must set up request filtering to allow them. This is done by editing the request filtering feature in the IIS Manager on your distribution point computers.

Additionally, the following file name extensions are used by Configuration Manager for packages and applications. Make sure that your request filtering configurations don't block these file extensions:

- .PCK
- .PKG
- .STA

- .TAR

For example, source files for a software deployment might include a folder named **bin** or have a file that has the **.mdb** file name extension.

- By default, IIS request filtering blocks access to these elements (**bin** is blocked as a Hidden Segment and **.mdb** is blocked as a file name extension).
- When you use the default IIS configuration on a distribution point, clients that use BITS fail to download this software deployment from the distribution point and indicate that they're waiting for content.
- To let the clients download this content, on each applicable distribution point, edit **Request Filtering** in IIS Manager to allow access to the file extensions and folders that are in the packages and applications that you deploy.

> **IMPORTANT**
>
> Edits to the request filter can increase the attack surface of the computer.
>
> - Edits that you make at the server level apply to all websites on the server.
>   - Edits that you make to individual websites apply to only that website.
>
> The security best practice is to run Configuration Manager on a dedicated web server. If you must run other applications on the web server, use a custom website for Configuration Manager. For information, see Websites for site system servers.

HTTP verbs

Management points: To ensure that clients can successfully communicate with a management point, on the management point server ensure the following HTTP verbs are allowed:

- GET
- POST
- CCM_POST
- HEAD
- PROPFIND

Distribution points: Distribution points require that the following HTTP verbs as allowed:

- GET
- HEAD
- PROPFIND

For more information, see Configure request filtering in IIS.

Websites for site system servers in System Center Configuration Manager

9/11/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Several Configuration Manager site system roles require the use of Microsoft Internet Information Services (IIS) and use the default IIS website to host site system services. When you must run other web applications on the same server and settings are not compatible with Configuration Manager, consider using a custom website for Configuration Manager.

> **TIP**
> A security best practice is to dedicate a server for the Configuration Manager site systems that require IIS. When you run other applications on a Configuration Manager site system, you increase the attack surface of that computer.

What to know before choosing to use custom websites

By default, site system roles use the **Default Web Site** in IIS. This is set up automatically when the site system role installs. However, at primary sites, you can choose to use custom websites instead. When you use custom websites:

- Custom websites are enabled for the entire site instead of for individual site system servers or roles.
- At primary sites, each computer that will host an applicable site system role must be set up with a custom website named **SMSWEB**. Until you create this website and set up site system roles on that computer to use the custom website, clients might not be able to communicate with site system roles on that computer.
- Because secondary sites are automatically set up to use a custom website when their primary parent site is set up to do so, you must also create custom websites in IIS on each secondary site system server that requires IIS.

Prerequisites for using custom websites:

Before you enable the option to use custom websites at a site, you must:

- Create a custom website named **SMSWEB** in IIS on each site system server that requires IIS. Do this at the primary site and at any child secondary sites.
- Set up the custom website to respond to the same port that you set up for Configuration Manager client communication (client request port).
- For each custom or default website that uses a custom folder, place a copy of the default document type that you use in the root folder that hosts the website. For example, on a Windows Server 2008 R2 computer that has default configurations, **iisstart.htm** is one of several default document types that are available. You can find this file in the root of the default website and then place a copy of this file (or a copy of the default document type that you use) in the root folder that hosts the SMSWEB custom website. For more about default document types, see Default Document <defaultDocument> for IIS.

About IIS requirements: The following site system roles require IIS and a website to host the site system services:

- Application Catalog web service point

- Application Catalog website point
- Distribution point
- Enrollment point
- Enrollment proxy point
- Fallback status point
- Management point
- Software update point
- State migration point

Additional considerations:

- When a primary site has custom websites enabled, clients that are assigned to that site are directed to communicate with the custom websites instead of the default websites on applicable site system servers
- If you use custom websites for one primary site, consider custom websites for all primary sites in your hierarchy to ensure that clients can successfully roam within the hierarchy. (Roaming is when a client computer moves to a new network segment that is managed by a different site. Roaming can affect resources that a client can access locally instead of across a WAN link).
- Site system roles that use IIS but do not accept client connections, like the reporting services point, also use the SMSWEB website instead of the default website.
- Custom websites require you to assign port numbers that differ from those that the computer's default website uses. A default website and custom website cannot run at the same time if both websites try to use the same TCP/IP ports.
- The TCP/IP ports that you set up in IIS for the custom website must match the client request ports for the site.

Switch between default and custom websites

Although you can check or uncheck the box for using custom websites at a primary site at any time (the box is on the General tab of the site's Properties), plan carefully before you make this change. When this configuration changes, all applicable site system roles at the primary site and child secondary sites must uninstall and then reinstall:

The following roles **reinstall automatically**:

- Management point
- Distribution point
- Software update point
- Fallback status point
- State migration point

The following roles must be **manually reinstalled**:

- Application Catalog web service point
- Application Catalog website point
- Enrollment point

- Enrollment proxy point

Additionally:

- When you change from the default website to use a custom website, Configuration Manager does not remove the old virtual directories. If you want to remove the files that Configuration Manager used, you must manually delete the virtual directories that were created under the default website.
- If you change the site to use custom websites, clients that are already assigned to the site must then be reconfigured to use the new client request ports for the custom websites. See How to configure client communication ports in System Center Configuration Manager.

Set up custom websites

Because the steps to create a custom website vary for different operating system versions, refer to documentation for your operating system version for exact steps, but use the following information when applicable:

- The website name must be: **SMSWEB**.
- When you set up HTTPS, you must specify a SSL certificate before you can save the configuration.
- After you create the custom website, remove the custom website ports that you use from other websites in IIS:

  1. Edit the **Bindings** of the other websites to remove ports that match those that are assigned to the **SMSWEB** website.
  2. Start the **SMSWEB** website.
  3. Restart the **SMS_SITE_COMPONENT_MANAGER** service on the site server of the site.

CNG certificates overview

5/9/2019 • 2 minutes to read • Edit Online

Configuration Manager has limited support for Cryptography: Next Generation (CNG) certificates. Configuration Manager clients can use PKI client authentication certificate with private key in CNG Key Storage Provider (KSP). With KSP support, Configuration Manager clients support hardware-based private key, such as TPM KSP for PKI client authentication certificates.

Supported scenarios

You can use Cryptography API: Next Generation (CNG) certificate templates for the following scenarios:

- Client registration and communication with an HTTPS management point
- Software distribution and application deployment with an HTTPS distribution point
- Operating system deployment
- Client messaging SDK (with latest update) and ISV Proxy
- Cloud Management Gateway configuration

Starting with version 1802, use CNG certificates for the following HTTPS-enabled server roles:

- Management point
- Distribution point
- Software update point
- State migration point

Starting with version 1806, use CNG certificates for the following HTTPS-enabled server roles:

- Certificate registration point, including the NDES server with the Configuration Manager policy module

> **NOTE**
> CNG is backward compatible with Crypto API (CAPI). CAPI certificates continue to be supported even when CNG support is enabled on the client.

Unsupported scenarios

The following scenarios are currently not supported:

- The following server roles are not operational when installed in HTTPS mode with a CNG certificate bound to the web site in Internet Information Services (IIS):
  - Application catalog web service
  - Application catalog website
  - Enrollment point
  - Enrollment proxy point
- Software Center does not display applications and packages as available that are deployed to user or user group collections.
- Using CNG certificates to create a Cloud Distribution Point.
- If the NDES policy module is using a CNG certificate for client authentication, communication to the

certificate registration point fails.

  - This is supported starting in Configuration Manager version 1806.
- If you specify a CNG certificate when creating task sequence media, the wizard fails to create bootable media.

  - This is supported starting in Configuration Manager version 1806.

To use CNG certificates

To use CNG certificates, your certification authority (CA) needs to provide CNG certificate templates for target machines. Template details vary according to the scenario; however, the following properties are required:

- **Compatibility** tab
  - **Certificate Authority** must be Windows Server 2008 or later. (Windows Server 2012 is recommended.)
  - **Certificate recipient** must be Windows Vista/Server 2008 or later. (Windows 8/Windows Server 2012 is recommended.)
- **Cryptography** tab
  - **Provider Category** must be **Key Storage Provider**. (required)
  - **Request must use one of the following providers:** must be **Microsoft Software Key Storage Provider**.

> **NOTE**
> The requirements for your environment or organization may be different. Contact your PKI expert. The important point to consider is a certificate template must use a Key Storage Provider to take advantage of CNG.

For best results, we recommend building the Subject Name from Active Directory information. Use the DNS Name for **Subject name format** and include the DNS name in the alternate subject name. Otherwise, you must provide this information when the device enrolls into the certificate profile.

PKI certificate requirements for Configuration Manager

9/5/2019 • 14 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The public key infrastructure (PKI) certificates that you might require for Configuration Manager are listed in the following tables. This information assumes basic knowledge of PKI certificates. For more information, see Step-by-step example deployment of the PKI certificates for Configuration Manager: Windows Server 2008 Certification Authority.

For more about Active Directory Certificate Services, see the following documentation:

- For Windows Server 2012: Active Directory Certificate Services Overview
- For Windows Server 2008: Active Directory Certificate Services in Windows Server 2008

For information about using Cryptography API: Next Generation (CNG) certificates with Configuration Manager, see CNG certificates overview.

> **IMPORTANT**
>
> Configuration Manager supports Secure Hash Algorithm 2 (SHA-2) certificates. SHA-2 certificates bring an important security advantage. Therefore, we recommend the following:
>
> - Issue new server and client authentication certificates that are signed with SHA-2, which includes SHA-256 and SHA-512, among others.
> - All internet-facing services should use a SHA-2 certificate. For example, if you purchase a public certificate for use with a cloud management gateway, make sure that you purchase a SHA-2 certificate.
>
> Effective February 14, 2017, Windows no longer trusts certain certificates signed with SHA-1. In general, we recommend that you issue new server and client authentication certificates signed with SHA-2 (which includes SHA-256 and SHA-512, among others). Additionally, we recommend that any internet-facing services use a SHA-2 certificate. For example, if you purchase a public certificate for use with a cloud management gateway, make sure that you purchase a SHA-2 certificate."
>
> In most cases, the change to SHA-2 certificates has no impact on operations. For more information, see Windows Enforcement of SHA1 certificates.

You can use any PKI to create, deploy, and manage these certificates, with the following exceptions:

- Client certificates that Configuration Manager enrolls on mobile devices and Mac computers
- Certificates that Microsoft Intune automatically creates to manage mobile devices

When you use Active Directory Certificate Services and certificate templates, this Microsoft PKI solution can ease the management of certificates. Use the **Microsoft certificate template to use** column in the following tables to identify the certificate template that most closely matches the certificate requirements. Only an enterprise certification authority that runs on the Enterprise Edition or Datacenter Edition of the server operating system, like Windows Server 2008 Enterprise and Windows Server 2008 Datacenter, can use template-based certificates.

Use the following sections to view the certificate requirements.

PKI Certificates for Servers

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
Site systems that run internet Information Services (IIS) and that are set up for HTTPS client connections: • Management point • Distribution point • Software update point • State migration point • Enrollment point • Enrollment proxy point • Application Catalog web service point • Application Catalog website point • A certificate registration point	Server authentication	**Web Server**	**Enhanced Key Usage** value must contain **Server Authentication (1.3.6.1.5.5.7.3.1)**. If the site system accepts connections from the internet, the Subject Name or Subject Alternative Name must contain the internet fully qualified domain name (FQDN). If the site system accepts connections from the intranet, the Subject Name or Subject Alternative Name must contain either the intranet FQDN (recommended) or the computer's name, depending on how the site system is set up. If the site system accepts connections from both the internet and the intranet, both the internet FQDN and the intranet FQDN (or computer name) must be specified by using the ampersand (&) symbol delimiter between the two names. **Note:** When the software update point accepts client connections from the internet only, the certificate must contain both the internet FQDN and the intranet FQDN. The SHA-2 hash algorithm is supported. Configuration Manager does not	This certificate must reside in the Personal store in the Computer certificate store. This web server certificate is used to authenticate these servers to the client and to encrypt all data that's transferred between the client and these servers by using Secure Sockets Layer (SSL).

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION TO THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
			specify a maximum supported key length for this certificate. Consult your PKI and IIS documentation for any key-size related issues for this certificate.	
Cloud-based distribution point	Server authentication	**Web Server**	**Enhanced Key Usage** value must contain **Server Authentication (1.3.6.1.5.5.7.3.1)**. The Subject Name must contain a customer-defined service name and domain name in an FQDN format as the Common Name for the specific instance of the cloud-based distribution point. The private key must be exportable. The SHA-2 hash algorithm is supported. Supported key lengths: 2,048 bits.	This service certificate is used to authenticate the cloud-based distribution point service to Configuration Manager clients and to encrypt all data transferred between them by using Secure Sockets Layer (SSL). This certificate must be exported in a Public Key Certificate Standard (PKCS #12) format, and the password must be known so that it can be imported when you create a cloud-based distribution point. **Note:** This certificate is used in conjunction with the Windows Azure management certificate.
Site system servers that run Microsoft SQL Server	Server authentication	**Web server**	**Enhanced Key Usage** value must contain **Server Authentication (1.3.6.1.5.5.7.3.1)**. The Subject Name must contain the intranet fully qualified domain name (FQDN). The SHA-2 hash algorithm is supported. Maximum supported key length is 2,048 bits.	This certificate must be in the Personal store in the Computer certificate store. Configuration Manager automatically copies it to the Trusted People Store for servers in the Configuration Manager hierarchy that might have to establish trust with the server. These certificates are used for server-to-server authentication.

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
SQL Server cluster: Site system servers that run Microsoft SQL Server	Server authentication	**Web server**	**Enhanced Key Usage** value must contain **Server Authentication (1.3.6.1.5.5.7.3.1)**. The Subject Name must contain the intranet fully qualified domain name (FQDN) of the cluster. The private key must be exportable. The certificate must have a validity period of at least two years when you configure Configuration Manager to use the SQL Server cluster. The SHA-2 hash algorithm is supported. Maximum supported key length is 2,048 bits.	After you have requested and installed this certificate on one node in the cluster, export the certificate and import it to each additional node in the SQL Server cluster. This certificate must be in the Personal store in the Computer certificate store. Configuration Manager automatically copies it to the Trusted People Store for servers in the Configuration Manager hierarchy that might have to establish trust with the server. These certificates are used for server-to-server authentication.
Site system monitoring for the following site system roles: • Management point • State migration point	Client authentication	**Workstation Authentication**	**Enhanced Key Usage** value must contain **Client Authentication (1.3.6.1.5.5.7.3.2)**. Computers must have a unique value in the Subject Name field or in the Subject Alternative Name field. **Note:** If you are using multiple values for the Subject Alternative Name, only the first value is used. The SHA-2 hash algorithm is supported. Maximum supported key length is 2,048 bits.	This certificate is required on the listed site system servers, even if the Configuration Manager client is not installed. This setup enables the health of these site system roles to be monitored and reported to the site. The certificate for these site systems must reside in the Personal store of the Computer certificate store.

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
Servers running the Configuration Manager Policy Module with the Network Device Enrollment Service role service	Client authentication	**Workstation Authentication**	**Enhanced Key Usage** value must contain **Client Authentication (1.3.6.1.5.5.7.3.2)**. There are no specific requirements for the certificate Subject or Subject Alternative Name (SAN). You can use the same certificate for multiple servers running the Network Device Enrollment Service. SHA-2 and SHA-3 hash algorithms are supported. Supported key lengths: 1,024 bits and 2,048 bits.	
Site systems that have a distribution point installed	Client authentication	**Workstation Authentication**	**Enhanced Key Usage** value must contain **Client Authentication (1.3.6.1.5.5.7.3.2)**. There are no specific requirements for the certificate Subject or Subject Alternative Name (SAN). You can use the same certificate for multiple distribution points. However, it's a good idea to use a different certificate for each distribution point. The private key must be exportable. The SHA-2 hash algorithm is supported. Maximum supported key length is 2,048 bits.	This certificate has two purposes: • It authenticates the distribution point to an HTTPS-enabled management point before the distribution point sends status messages. • When the **Enable PXE support for clients** distribution point option is selected, the certificate is sent to computers. If task sequences in the operating system deployment process include client

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
				actions like client policy retrieval or sending inventory information, the client computers can connect to a HTTPS-enabled management point during the deployment of the operating system. This certificate is used for the duration of the operating system deployment process only and is not installed on the client. Because of this temporary use, the same certificate can be used for every operating system deployment if you do not want to use multiple client certificates. This certificate must be exported in a Public Key Certificate Standard (PKCS #12) format. The password must be known so that it can be imported into the distribution point properties. **Note:** The requirements for this certificate are the same as the client certificate for boot images that deploy operating systems. Because the requirements are the same, you can use the same certificate file.

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
Site system server that runs the Microsoft Intune connector	Client authentication	Not applicable: Intune automatically creates this certificate.	**Enhanced Key Usage** value contains **Client Authentication (1.3.6.1.5.5.7.3.2)**. Three custom extensions uniquely identify the customer's Intune subscription. The key size is 2,048 bits and uses the SHA-1 hash algorithm. **Note:** You cannot change these settings. This information is provided for informational purposes only.	This certificate is automatically requested and installed to the Configuration Manager database when you subscribe to Microsoft Intune. When you install the Microsoft Intune connector, this certificate is then installed on the site system server that runs the Microsoft Intune connector. It is installed in the Computer certificate store. This certificate is used to authenticate the Configuration Manager hierarchy to Microsoft Intune by using the Microsoft Intune connector. All data that is transferred between them uses Secure Sockets Layer (SSL).

Proxy web servers for internet-based client management

If the site supports internet-based client management, and you are using a proxy web server by using SSL termination (bridging) for incoming internet connections, the proxy web server has the certificate requirements listed in the following table.

> **NOTE**
>
> If you are using a proxy web server without SSL termination (tunneling), no additional certificates are required on the proxy web server.

NETWORK INFRASTRUCTURE COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER

NETWORK INFRASTRUCTURE COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
Proxy web server accepting client connections over the internet	Server authentication and client authentication	1. **Web Server** 2. **Workstation Authentication**	internet FQDN in the Subject Name field or in the Subject Alternative Name field. If you are using Microsoft certificate templates, the Subject Alternative Name is available with the workstation template only. The SHA-2 hash algorithm is supported.	This certificate is used to authenticate the following servers to internet clients and to encrypt all data transferred between the client and this server by using SSL: • Internet-based management point • Internet-based distribution point • Internet-based software update point The client authentication is used to bridge client connections between the Configuration Manager clients and the internet-based site systems.

PKI certificates for clients

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
Windows client computers	Client authentication	**Workstation Authentication**	**Enhanced Key Usage** value must contain **Client Authentication (1.3.6.1.5.5.7.3.2)**. Client computers must have a unique value in the Subject Name field or in the Subject Alternative Name field. **Note:** If you are using multiple values for the Subject Alternative Name, only the first value is used. The SHA-2 hash algorithm is supported. Maximum supported key length is 2,048 bits.	By default, Configuration Manager looks for computer certificates in the Personal store in the Computer certificate store. Except for the software update point and the Application Catalog website point, this certificate authenticates the client to site system servers that run IIS and that are set up to use HTTPS.
Mobile device clients	Client authentication	**Authenticated Session**	**Enhanced Key Usage** value must contain **Client Authentication (1.3.6.1.5.5.7.3.2)**. SHA-1 Maximum supported key length is 2,048 bits. **Notes:** • These certificates must be in Distinguished Encoding Rules (DER) encoded binary X.509 format. • Base64 encoded X.509 format is not supported.	This certificate authenticates the mobile device client to the site system servers that it communicates with, like management points and distribution points.
Boot images for deploying operating systems	Client authentication	**Workstation Authentication**	**Enhanced Key Usage** value must contain **Client**	The certificate is used if task sequences in the operating system

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
			Authentication (1.3.6.1.5.5.7.3.2). There are no specific requirements for the certificate Subject Name field or Subject Alternative Name (SAN), and you can use the same certificate for all boot images. The private key must be exportable. The SHA-2 hash algorithm is supported. Maximum supported key length is 2,048 bits.	deployment process include client actions like client policy retrieval or sending inventory information. This certificate is used for the duration of the operating system deployment process only and is not installed on the client. Because of this temporary use, the same certificate can be used for every operating system deployment if you do not want to use multiple client certificates. This certificate must be exported in a Public Key Certificate Standard (PKCS #12) format, and the password must be known so that it can be imported to the Configuration Manager boot images. This certificate is temporary for the task sequence and not used to install the client. When you have an environment with HTTPS only, the client must have a valid certificate for the client to communicate with the site and for the deployment to continue. The client can automatically generate a certificate when the client is joined to Active Directory, or you can install a client certificate by using another method. **Note:** The requirements for this certificate are the same as the server certificate for site systems that have a distribution point installed. Because the

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
Mac client computers	Client authentication	For Configuration Manager enrollment: **Authenticated Session** For certificate installation independent from Configuration Manager: **Workstation Authentication**	**Enhanced Key Usage** value must contain **Client Authentication (1.3.6.1.5.5.7.3.2)**. For Configuration Manager that creates a User certificate, the certificate Subject value is automatically populated with the user name of the person who enrolls the Mac computer. For certificate installation that does not use Configuration Manager enrollment but deploys a Computer certificate independently from Configuration Manager, the certificate Subject value must be unique. For example, specify the FQDN of the computer. The Subject Alternative Name field is not supported. The SHA-2 hash algorithm is supported. Maximum supported key length is 2,048 bits.	This certificate authenticates the Mac client computer to the site system servers that it communicates with, like management points and distribution points.

requirements are the same, you can use the same certificate file.

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
Linux and UNIX client computers	Client authentication	**Workstation Authentication**	**Enhanced Key Usage** value must contain **Client Authentication (1.3.6.1.5.5.7.3.2)**. The Subject Alternative Name field is not supported. The private key must be exportable. SHA-2 hash algorithm is supported if the operating system of the client supports SHA-2. For more information, see the About Linux and UNIX Operating Systems That do not Support SHA-256 section in Planning for client deployment to Linux and UNIX computers in Configuration Manager. Supported key lengths: 2,048 bits. **Note:** These certificates must be in Distinguished Encoding Rules (DER) encoded binary X.509 format. Base64 encoded X.509 format is not supported.	This certificate authenticates the Linux or UNIX client computer to the site system servers that it communicates with, like management points and distribution points. This certificate must be exported in a Public Key Certificate Standard (PKCS#12) format, and the password must be known so you can specify it to the client when you specify the PKI certificate. For additional information, see the Planning for Security and Certificates for Linux and UNIX Servers section in Planning for client deployment to Linux and UNIX computers in Configuration Manager.

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
Root certification authority (CA) certificates for the following scenarios: • Operating system deployment • Mobile device enrollment • Client certificate authentication	Certificate chain to a trusted source	Not applicable.	Standard root CA certificate.	The root CA certificate must be provided when clients have to chain the certificates of the communicating server to a trusted source. This applies in the following scenarios: • When you deploy an operating system, and task sequences run that connect the client computer to a management point that is set up to use HTTPS. • When you enroll a mobile device to be managed by Configuration Manager. In addition, the root CA certificate for clients must be provided if the client certificates are issued by a different CA hierarchy than the CA hierarchy that issued the management point certificate.

CONFIGURATION MANAGER COMPONENT	CERTIFICATE PURPOSE	MICROSOFT CERTIFICATE TEMPLATE TO USE	SPECIFIC INFORMATION IN THE CERTIFICATE	HOW THE CERTIFICATE IS USED IN CONFIGURATION MANAGER
Mobile devices that are enrolled by Microsoft Intune	Client authentication	Not applicable: Intune automatically creates this certificate.	**Enhanced Key Usage** value contains **Client Authentication (1.3.6.1.5.5.7.3.2)**. Three custom extensions uniquely identify the customer Intune subscription. Users can supply the certificate Subject value during enrollment. However, Intune does not use this value to identify the device. The key size is 2,048 bits and uses the SHA-1 hash algorithm. **Note:** You cannot change these settings. This information is provided for informational purposes only.	This certificate is automatically requested and installed when authenticated users enroll their mobiles devices by using Microsoft Intune. The resulting certificate on the device resides in the Computer store and authenticates the enrolled mobile device to Intune, so that it can then be managed. Because of the custom extensions in the certificate, authentication is restricted to the Intune subscription that has been established for the organization.

Step-by-step example deployment of the PKI certificates for Configuration Manager: Windows Server 2008 certification authority

8/30/2019 • 29 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This step-by-step example deployment, which uses a Windows Server 2008 certification authority (CA), has procedures that show you how to create and deploy the public key infrastructure (PKI) certificates that Configuration Manager uses. These procedures use an enterprise certification authority (CA) and certificate templates. The steps are appropriate for a test network only, as a proof of concept.

Because there's no single method of deployment for the required certificates, consult your particular PKI deployment documentation for the required procedures and best practices to deploy the required certificates for a production environment. For more about the certificate requirements, see PKI certificate requirements for Configuration Manager.

> **TIP**
> You can adapt the instructions in this topic for operating systems that aren't documented in the Test Network Requirements section. However, if you are running the issuing CA on Windows Server 2012, you're not prompted for the certificate template version. Instead, specify this on the **Compatibility** tab of the template properties:
>
> - **Certification Authority**: **Windows Server 2003**
>   - **Certificate recipient**: **Windows XP / Server 2003**

Test network requirements

The step-by-step instructions have the following requirements:

- The test network is running Active Directory Domain Services with Windows Server 2008, and it is installed as a single domain, single forest.
- You have a member server running Windows Server 2008 Enterprise Edition, which has the Active Directory Certificate Services role installed on it, and it is set up as an enterprise root certification authority (CA).
- You have one computer that has Windows Server 2008 (Standard Edition or Enterprise Edition, R2 or later) installed on it, that computer is designated as a member server, and Internet Information Services (IIS) is installed on it. This computer will be the Configuration Manager site system server that you will configure with an intranet fully qualified domain name (FQDN) to support client connections on the intranet and an internet FQDN if you must support mobile devices that are enrolled by Configuration Manager and clients on the internet.
- You have one Windows Vista client that has the latest service pack installed, and this computer is set up with a computer name that comprises ASCII characters and is joined to the domain. This computer will be a Configuration Manager client computer.
- You can sign in with a root domain administrator account or an enterprise domain administrator account and use this account for all procedures in this example deployment.

Overview of the certificates

The following table lists the types of PKI certificates that might be required for Configuration Manager and describes how they are used.

CERTIFICATE REQUIREMENT	CERTIFICATE DESCRIPTION
Web server certificate for site systems that run IIS	This certificate is used to encrypt data and authenticate the server to clients. It must be installed externally from Configuration Manager on site systems servers that run Internet Information Services (IIS) and that are set up in Configuration Manager to use HTTPS. For the steps to set up and install this certificate, see Deploy the web server certificate for site systems that run IIS in this topic.
Service certificate for clients to connect to cloud-based distribution points	For the steps to configure and install this certificate, see Deploy the service certificate for cloud-based distribution points in this topic. **Important:** This certificate is used in conjunction with the Windows Azure management certificate. For more about the management certificate, see How to Create a Management Certificate and How to Add a Management Certificate to a Windows Azure Subscription in the Windows Azure Platform section of the MSDN Library.
Client certificate for Windows computers	This certificate is used to authenticate Configuration Manager client computers to site systems that are set up to use HTTPS. It can also be used for management points and state migration points to monitor their operational status when they are set up to use HTTPS. It must be installed externally from Configuration Manager on computers. For the steps to set up and install this certificate, see Deploy the client certificate for Windows computers in this topic.
Client certificate for distribution points	This certificate has two purposes: The certificate is used to authenticate the distribution point to an HTTPS-enabled management point before the distribution point sends status messages. When the **Enable PXE support for clients** distribution point option is selected, the certificate is sent to computers that PXE boot so that they can connect to a HTTPS-enabled management point during the deployment of the operating system. For the steps to set up and install this certificate, see Deploy the client certificate for distribution points in this topic.

CERTIFICATE REQUIREMENT	CERTIFICATE DESCRIPTION
Enrollment certificate for mobile devices	This certificate is used to authenticate Configuration Manager mobile device clients to site systems that are set up to use HTTPS. It must be installed as part of mobile device enrollment in Configuration Manager, and you choose the configured certificate template as a mobile device client setting. For the steps to set up this certificate, see Deploy the enrollment certificate for mobile devices in this topic.
Client certificate for Mac computers	You can request and install this certificate from a Mac computer when you use Configuration Manager enrollment and choose the configured certificate template as a mobile device client setting. For the steps to set up this certificate, see Deploy the client certificate for Mac computers in this topic.

Deploy the web server certificate for site systems that run IIS

This certificate deployment has the following procedures:

- Create and issue the web server certificate template on the certification authority
- Request the web server certificate
- Configure IIS to use the web server certificate

Create and issue the web server certificate template on the certification authority

This procedure creates a certificate template for Configuration Manager site systems and adds it to the certification authority.

To create and issue the web server certificate template on the certification authority

1. Create a security group named **ConfigMgr IIS Servers** that has the member servers to install Configuration Manager site systems that will run IIS.
2. On the member server that has Certificate Services installed, in the Certification Authority console, right-click **Certificate Templates** and then choose **Manage** to load the **Certificate Templates** console.
3. In the results pane, right-click the entry that has **Web Server** in the **Template Display Name** column, and then choose **Duplicate Template**.
4. In the **Duplicate Template** dialog box, ensure that **Windows 2003 Server, Enterprise Edition** is selected, and then choose **OK**.

   > **IMPORTANT**
   > Do not select **Windows 2008 Server, Enterprise Edition**.

5. In the **Properties of New Template** dialog box, on the **General** tab, enter a template name, like **ConfigMgr Web Server Certificate**, to generate the web certificates that will be used on Configuration Manager site systems.
6. Choose the **Subject Name** tab, and make sure that **Supply in the request** is selected.
7. Choose the **Security** tab, and then remove the **Enroll** permission from the **Domain Admins** and **Enterprise Admins** security groups.

8. Choose **Add**, enter **ConfigMgr IIS Servers** in the text box, and then choose **OK**.
9. Choose the **Enroll** permission for this group, and do not clear the **Read** permission.
10. Choose **OK**, and then close the **Certificate Templates Console**.
11. In the Certification Authority console, right-click **Certificate Templates**, choose **New**, and then choose **Certificate Template to Issue**.
12. In the **Enable Certificate Templates** dialog box, choose the new template that you just created, **ConfigMgr Web Server Certificate**, and then choose **OK**.
13. If you do not need to create and issue more certificates, close **Certification Authority**.

Request the web server certificate

This procedure lets you specify the intranet and internet FQDN values that will be set up in the site system server properties and then installs the web server certificate on to the member server that runs IIS.

To request the web server certificate

1. Restart the member server that runs IIS to ensure that the computer can access the certificate template that you created by using the **Read** and **Enroll** permissions that you configured.
2. Choose **Start**, choose **Run**, and then type **mmc.exe.** In the empty console, choose **File**, and then choose **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog box, choose **Certificates** from the list of **Available snap-ins**, and then choose **Add**.
4. In the **Certificate snap-in** dialog box, choose **Computer account**, and then choose **Next**.
5. In the **Select Computer** dialog box, ensure that **Local computer: (the computer this console is running on)** is selected, and then choose **Finish**.
6. In the **Add or Remove Snap-ins** dialog box, choose **OK**.
7. In the console, expand **Certificates (Local Computer)**, and then choose **Personal**.
8. Right-click **Certificates**, choose **All Tasks**, and then choose **Request New Certificate**.
9. On the **Before You Begin** page, choose **Next**.
10. If you see the **Select Certificate Enrollment Policy** page, choose **Next**.
11. On the **Request Certificates** page, identify the **ConfigMgr Web Server Certificate** from the list of available certificates, and then choose **More information is required to enroll for this certificate. Click here to configure settings**.
12. In the **Certificate Properties** dialog box, in the **Subject** tab, do not make any changes to **Subject name**. This means that the **Value** box for the **Subject name** section remains blank. Instead, from the **Alternative name** section, choose the **Type** drop-down list, and then choose **DNS**.
13. In the **Value** box, specify the FQDN values that you will specify in the Configuration Manager site system properties, and then choose **OK** to close the **Certificate Properties** dialog box.

    Examples:

    - If the site system will only accept client connections from the intranet, and the intranet FQDN of the site system server is **server1.internal.contoso.com**, enter **server1.internal.contoso.com**, and then choose **Add**.
    - If the site system will accept client connections from the intranet and the internet, and the intranet FQDN of the site system server is **server1.internal.contoso.com** and the internet FQDN of the site

system server is **server.contoso.com**:

a. Enter **server1.internal.contoso.com**, and then choose **Add**.

b. Enter **server.contoso.com**, and then choose **Add**.

> **NOTE**
> You can specify the FQDNs for Configuration Manager in any order. However, check that all devices that will use the certificate, such as mobile devices and proxy web servers, can use a certificate subject alternative name (SAN) and multiple values in the SAN. If devices have limited support for SAN values in certificates, you might have to change the order of the FQDNs or use the Subject value instead.

14. On the **Request Certificates** page, choose **ConfigMgr Web Server Certificate** from the list of available certificates, and then choose **Enroll**.
15. On the **Certificates Installation Results** page, wait until the certificate is installed, and then choose **Finish**.
16. Close **Certificates (Local Computer)**.

Configure IIS to use the web server certificate

This procedure binds the installed certificate to the IIS **Default Web Site**.

To set up IIS to use the web server certificate

1. On the member server that has IIS installed, choose **Start**, choose **Programs**, choose **Administrative Tools**, and then choose **Internet Information Services (IIS) Manager**.
2. Expand **Sites**, right-click **Default Web Site**, and then choose **Edit Bindings**.
3. Choose the **https** entry, and then choose **Edit**.
4. In the **Edit Site Binding** dialog box, select the certificate that you requested by using the ConfigMgr Web Server Certificates template, and then choose **OK**.

   > **NOTE**
   > If you are not sure which is the correct certificate, choose one, and then choose **View**. This lets you compare the selected certificate details to the certificates in the Certificates snap-in. For example, the Certificates snap-in shows the certificate template that was used to request the certificate. You can then compare the certificate thumbprint of the certificate that was requested by using the ConfigMgr Web Server Certificates template to the certificate thumbprint of the certificate currently selected in the **Edit Site Binding** dialog box.

5. Choose **OK** in the **Edit Site Binding** dialog box, and then choose **Close**.
6. Close **Internet Information Services (IIS) Manager**.

   The member server is now set up with a Configuration Manager web server certificate.

> **IMPORTANT**
> When you install the Configuration Manager site system server on this computer, make sure that you specify the same FQDNs in the site system properties as you specified when you requested the certificate.

Deploy the service certificate for cloud-based distribution points

This certificate deployment has the following procedures:

- Create and issue a custom web server certificate template on the certification authority
- Request the custom web server certificate
- Export the custom web server certificate for cloud-based distribution points

Create and issue a custom web server certificate template on the certification authority

This procedure creates a custom certificate template that is based on the web server certificate template. The certificate is for Configuration Manager cloud-based distribution points and the private key must be exportable. After the certificate template is created, it is added to the certification authority.

> **NOTE**
>
> This procedure uses a different certificate template from the web server certificate template that you created for site systems that run IIS. Although both certificates require server authentication capability, the certificate for cloud-based distribution points requires you to enter a custom-defined value for the Subject Name and the private key must be exported. As a security best practice, do not set up certificate templates so that the private key can be exported unless this configuration is required. The cloud-based distribution point requires this configuration because you must import the certificate as a file, rather than choose it from the certificate store.
>
> When you create a new certificate template for this certificate, you can restrict the computers that can request a certificate whose private key can be exported. On a production network, you might also consider adding the following changes for this certificate:
>
> - Require approval to install the certificate for additional security.
>   - Increase the certificate validity period. Because you must export and import the certificate each time before it expires, an increase of the validity period reduces how often you must repeat this procedure. However, an increase of the validity period also decreases the security of the certificate because it provides more time for an attacker to decrypt the private key and steal the certificate.
>   - Use a custom value in the certificate Subject Alternative Name (SAN) to help identify this certificate from standard web server certificates that you use with IIS.

To create and issue the custom web server certificate template on the certification authority

1. Create a security group named **ConfigMgr Site Servers** that has the member servers to install Configuration Manager primary site servers that will manage cloud-based distribution points.
2. On the member server that is running the Certification Authority console, right-click **Certificate Templates**, and then choose **Manage** to load the Certificate Templates management console.
3. In the results pane, right-click the entry that has **Web Server** in the **Template Display Name** column, and then choose **Duplicate Template**.
4. In the **Duplicate Template** dialog box, ensure that **Windows 2003 Server, Enterprise Edition** is selected, and then choose **OK**.

   > **IMPORTANT**
   >
   > Do not select **Windows 2008 Server, Enterprise Edition**.

5. In the **Properties of New Template** dialog box, on the **General** tab, enter a template name, like **ConfigMgr Cloud-Based Distribution Point Certificate**, to generate the web server certificate for cloud-based distribution points.
6. Choose the **Request Handling** tab, and then choose **Allow private key to be exported**.
7. Choose the **Security** tab, and then remove the **Enroll** permission from the **Enterprise Admins** security group.

8. Choose **Add**, enter **ConfigMgr Site Servers** in the text box, and then choose **OK**.
9. Select the **Enroll** permission for this group, and do not clear the **Read** permission.

   > **NOTE**
   > Ensure that **Minimum key size** on the **Cryptography** tab has been set to **2048**

10. Choose **OK**, and then close **Certificate Templates Console**.
11. In the Certification Authority console, right-click **Certificate Templates**, choose **New**, and then choose **Certificate Template to Issue**.
12. In the **Enable Certificate Templates** dialog box, choose the new template that you just created, **ConfigMgr Cloud-Based Distribution Point Certificate**, and then choose **OK**.
13. If you do not have to create and issue more certificates, close **Certification Authority**.

Request the custom web server certificate

This procedure requests and then installs the custom web server certificate on the member server that will run the site server.

To request the custom web server certificate

1. Restart the member server after you create and configure the **ConfigMgr Site Servers** security group to ensure that the computer can access the certificate template that you created by using the **Read** and **Enroll** permissions that you configured.
2. Choose **Start**, choose **Run**, and then enter **mmc.exe.** In the empty console, choose **File**, and then choose **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog box, choose **Certificates** from the list of **Available snap-ins**, and then choose **Add**.
4. In the **Certificate snap-in** dialog box, choose **Computer account**, and then choose **Next**.
5. In the **Select Computer** dialog box, ensure that **Local computer: (the computer this console is running on)** is selected, and then choose **Finish**.
6. In the **Add or Remove Snap-ins** dialog box, choose **OK**.
7. In the console, expand **Certificates (Local Computer)**, and then choose **Personal**.
8. Right-click **Certificates**, choose **All Tasks**, and then choose **Request New Certificate**.
9. On the **Before You Begin** page, choose **Next**.
10. If you see the **Select Certificate Enrollment Policy** page, choose **Next**.
11. On the **Request Certificates** page, identify the **ConfigMgr Cloud-Based Distribution Point Certificate** from the list of available certificates, and then choose **More information is required to enroll for this certificate. choose here to configure settings**.
12. In the **Certificate Properties** dialog box, in the **Subject** tab, for the **Subject name**, choose **Common name** as the **Type**.
13. In the **Value** box, specify your choice of service name and your domain name by using an FQDN format. For example: **clouddp1.contoso.com**.

> **NOTE**
> Make the service name unique in your namespace. You will use DNS to create an alias (CNAME record) to map this service name to an automatically generated identifier (GUID) and an IP address from Windows Azure.

14. Choose **Add**, and then choose **OK** to close the **Certificate Properties** dialog box.
15. On the **Request Certificates** page, choose **ConfigMgr Cloud-Based Distribution Point Certificate** from the list of available certificates, and then choose **Enroll**.
16. On the **Certificates Installation Results** page, wait until the certificate is installed, and then choose **Finish**.
17. Close **Certificates (Local Computer)**.

Export the custom web server certificate for cloud-based distribution points

This procedure exports the custom web server certificate to a file, so that it can be imported when you create the cloud-based distribution point.

To export the custom web server certificate for cloud-based distribution points

1. In the **Certificates (Local Computer)** console, right-click the certificate that you just installed, choose **All Tasks**, and then choose **Export**.
2. In the Certificates Export Wizard, choose **Next**.
3. On the **Export Private Key** page, choose **Yes, export the private key**, and then choose **Next**.

   > **NOTE**
   > If this option is not available, the certificate has been created without the option to export the private key. In this scenario, you cannot export the certificate in the required format. You must set up the certificate template so that the private key can be exported, and then request the certificate again.

4. On the **Export File Format** page, ensure that the **Personal Information Exchange - PKCS #12 (.PFX)** option is selected.
5. On the **Password** page, specify a strong password to protect the exported certificate with its private key, and then choose **Next**.
6. On the **File to Export** page, specify the name of the file that you want to export, and then choose **Next**.
7. To close the wizard, choose **Finish** in the **Certificate Export Wizard** page, and then choose **OK** in the confirmation dialog box.
8. Close **Certificates (Local Computer)**.
9. Store the file securely and ensure that you can access it from the Configuration Manager console.

   The certificate is now ready to be imported when you create a cloud-based distribution point.

Deploy the client certificate for Windows computers

This certificate deployment has the following procedures:

- Create and issue the Workstation Authentication certificate template on the certification authority
- Configure autoenrollment of the Workstation Authentication template by using Group Policy
- Automatically enroll the Workstation Authentication certificate and verify its installation on computers

Create and issue the Workstation Authentication certificate template on the certification authority

This procedure creates a certificate template for Configuration Manager client computers and adds it to the certification authority.

To create and issue the Workstation Authentication certificate template on the certification authority

1. On the member server that is running the Certification Authority console, right-click **Certificate Templates**, and then choose **Manage** to load the Certificate Templates management console.
2. In the results pane, right-click the entry that has **Workstation Authentication** in the **Template Display Name** column, and then choose **Duplicate Template**.
3. In the **Duplicate Template** dialog box, ensure that **Windows 2003 Server, Enterprise Edition** is selected, and then choose **OK**.

   > **IMPORTANT**
   > Do not select **Windows 2008 Server, Enterprise Edition**.

4. In the **Properties of New Template** dialog box, on the **General** tab, enter a template name, like **ConfigMgr Client Certificate**, to generate the client certificates that will be used on Configuration Manager client computers.
5. Choose the **Security** tab, select the **Domain Computers** group, and then select the additional permissions of **Read** and **Autoenroll**. Do not clear **Enroll**.
6. Choose **OK**, and then close **Certificate Templates Console**.
7. In the Certification Authority console, right-click **Certificate Templates**, choose **New**, and then choose **Certificate Template to Issue**.
8. In the **Enable Certificate Templates** dialog box, choose the new template that you just created, **ConfigMgr Client Certificate**, and then choose **OK**.
9. If you do not need to create and issue more certificates, close **Certification Authority**.

Configure autoenrollment of the Workstation Authentication template by using Group Policy

This procedure sets up Group Policy to autoenroll the client certificate on computers.

To set up autoenrollment of the Workstation Authentication template by using Group Policy

1. On the domain controller, choose **Start**, choose **Administrative Tools**, and then choose **Group Policy Management**.
2. Go to your domain, right-click the domain, and then choose **Create a GPO in this domain, and Link it here**.

   > **NOTE**
   > This step uses the best practice of creating a new Group Policy for custom settings rather than editing the Default Domain Policy that is installed with Active Directory Domain Services. When you assign this Group Policy at the domain level, you will apply it to all computers in the domain. In a production environment, you can restrict the autoenrollment so that it enrolls on only selected computers. You can assign the Group Policy at an organizational unit level, or you can filter the domain Group Policy with a security group so that it applies only to the computers in the group. If you restrict autoenrollment, remember to include the server that is set up as the management point.

3. In the **New GPO** dialog box, enter a name, like **Autoenroll Certificates**, for the new Group Policy, and then choose **OK**.
4. In the results pane, on the **Linked Group Policy Objects** tab, right-click the new Group Policy, and then

choose **Edit**.

5. In the **Group Policy Management Editor**, expand **Policies** under **Computer Configuration**, and then go to **Windows Settings** / **Security Settings** / **Public Key Policies**.
6. Right-click the object type named **Certificate Services Client - Auto-enrollment**, and then choose **Properties**.
7. From the **Configuration Model** drop-down list, choose **Enabled**, choose **Renew expired certificates, update pending certificates, remove revoked certificates**, choose **Update certificates that use certificate templates**, and then choose **OK**.
8. Close **Group Policy Management**.

Automatically enroll the Workstation Authentication certificate and verify its installation on computers

This procedure installs the client certificate on computers and verifies the installation.

To automatically enroll the Workstation Authentication certificate and verify its installation on the client computer

1. Restart the workstation computer, and wait a few minutes before you sign in.

   > **NOTE**
   > Restarting a computer is the most reliable method of ensuring success with certificate autoenrollment.

2. Sign in with an account that has administrative privileges.
3. In the search box, enter **mmc.exe.**, and then press **Enter**.
4. In the empty management console, choose **File**, and then choose **Add/Remove Snap-in**.
5. In the **Add or Remove Snap-ins** dialog box, choose **Certificates** from the list of **Available snap-ins**, and then choose **Add**.
6. In the **Certificate snap-in** dialog box, choose **Computer account**, and then choose **Next**.
7. In the **Select Computer** dialog box, ensure that **Local computer: (the computer this console is running on)** is selected, and then choose **Finish**.
8. In the **Add or Remove Snap-ins** dialog box, choose **OK**.
9. In the console, expand **Certificates (Local Computer)**, expand **Personal**, and then choose **Certificates**.
10. In the results pane, confirm that a certificate has **Client Authentication** in the **Intended Purpose** column, and that **ConfigMgr Client Certificate** is in the **Certificate Template** column.
11. Close **Certificates (Local Computer)**.
12. Repeat steps 1 through 11 for the member server to verify that the server that will be set up as the management point also has a client certificate.

    The computer is now set up with a Configuration Manager client certificate.

Deploy the client certificate for distribution points

> **NOTE**
> This certificate can also be used for media images that do not use PXE boot, because the certificate requirements are the same.

This certificate deployment has the following procedures:

- Create and issue a custom Workstation Authentication certificate template on the certification authority
- Request the custom Workstation Authentication certificate
- Export the client certificate for distribution points

Create and issue a custom Workstation Authentication certificate template on the certification authority

This procedure creates a custom certificate template for Configuration Manager distribution points so that the private key can be exported and adds the certificate template to the certification authority.

> **NOTE**
>
> This procedure uses a different certificate template from the certificate template that you created for client computers. Although both certificates require client authentication capability, the certificate for distribution points requires that the private key is exported. As a security best practice, do not set up certificate templates so the private key can be exported unless this configuration is required. The distribution point requires this configuration because you must import the certificate as a file rather than choose it from the certificate store.
>
> When you create a new certificate template for this certificate, you can restrict the computers that can request a certificate whose private key can be exported. In our example deployment, this will be the security group that you previously created for Configuration Manager site system servers that run IIS. On a production network that distributes the IIS site system roles, consider creating a new security group for the servers that run distribution points so that you can restrict the certificate to just these site system servers. You might also consider adding the following modifications for this certificate:
>
> - Require approval to install the certificate for additional security.
>   - Increase the certificate validity period. Because you must export and import the certificate each time before it expires, an increase of the validity period reduces how often you must repeat this procedure. However, an increase of the validity period also decreases the security of the certificate because it provides more time for an attacker to decrypt the private key and steal the certificate.
>   - Use a custom value in the certificate Subject field or Subject Alternative Name (SAN) to help identify this certificate from standard client certificates. This can be particularly helpful if you will use the same certificate for multiple distribution points.

To create and issue the custom Workstation Authentication certificate template on the certification authority

1. On the member server that is running the Certification Authority console, right-click **Certificate Templates**, and then choose **Manage** to load the Certificate Templates management console.
2. In the results pane, right-click the entry that has **Workstation Authentication** in the **Template Display Name** column, and then choose **Duplicate Template**.
3. In the **Duplicate Template** dialog box, ensure that **Windows 2003 Server, Enterprise Edition** is selected, and then choose **OK**.

   > **IMPORTANT**
   >
   > Do not select **Windows 2008 Server, Enterprise Edition**.

4. In the **Properties of New Template** dialog box, on the **General** tab, enter a template name, like **ConfigMgr Client Distribution Point Certificate**, to generate the client authentication certificate for distribution points.
5. Choose the **Request Handling** tab, and then choose **Allow private key to be exported**.
6. Choose the **Security** tab, and then remove the **Enroll** permission from the **Enterprise Admins** security group.

7. Choose **Add**, enter **ConfigMgr IIS Servers** in the text box, and then choose **OK**.
8. Select the **Enroll** permission for this group, and do not clear the **Read** permission.
9. Choose **OK**, and then close **Certificate Templates Console**.
10. In the Certification Authority console, right-click **Certificate Templates**, choose **New**, and then choose **Certificate Template to Issue**.
11. In the **Enable Certificate Templates** dialog box, choose the new template that you just created, **ConfigMgr Client Distribution Point Certificate**, and then choose **OK**.
12. If you do not have to create and issue more certificates, close **Certification Authority**.

Request the custom Workstation Authentication certificate

This procedure requests and then installs the custom client certificate on to the member server that runs IIS and that will be set up as a distribution point.

To request the custom Workstation Authentication certificate

1. Choose **Start**, choose **Run**, and then enter **mmc.exe.** In the empty console, choose **File**, and then choose **Add/Remove Snap-in**.
2. In the **Add or Remove Snap-ins** dialog box, choose **Certificates** from the list of **Available snap-ins**, and then choose **Add**.
3. In the **Certificate snap-in** dialog box, choose **Computer account**, and then choose **Next**.
4. In the **Select Computer** dialog box, ensure that **Local computer: (the computer this console is running on)** is selected, and then choose **Finish**.
5. In the **Add or Remove Snap-ins** dialog box, choose **OK**.
6. In the console, expand **Certificates (Local Computer)**, and then choose **Personal**.
7. Right-click **Certificates**, choose **All Tasks**, and then choose **Request New Certificate**.
8. On the **Before You Begin** page, choose **Next**.
9. If you see the **Select Certificate Enrollment Policy** page, choose **Next**.
10. On the **Request Certificates** page, choose **ConfigMgr Client Distribution Point Certificate** from the list of available certificates, and then choose **Enroll**.
11. On the **Certificates Installation Results** page, wait until the certificate is installed, and then choose **Finish**.
12. In the results pane, confirm that a certificate has **Client Authentication** in the **Intended Purpose** column and that **ConfigMgr Client Distribution Point Certificate** is in the **Certificate Template** column.
13. Do not close **Certificates (Local Computer)**.

Export the client certificate for distribution points

This procedure exports the custom Workstation Authentication certificate to a file so that it can be imported in the distribution point properties.

To export the client certificate for distribution points

1. In the **Certificates (Local Computer)** console, right-click the certificate that you just installed, choose **All Tasks**, and then choose **Export**.
2. In the Certificates Export Wizard, choose **Next**.
3. On the **Export Private Key** page, choose **Yes, export the private key**, and then choose **Next**.

> **NOTE**
> If this option is not available, the certificate has been created without the option to export the private key. In this scenario, you cannot export the certificate in the required format. You must set up the certificate template so that the private key can be exported and then request the certificate again.

4. On the **Export File Format** page, ensure that the **Personal Information Exchange - PKCS #12 (.PFX)** option is selected.
5. On the **Password** page, specify a strong password to protect the exported certificate with its private key, and then choose **Next**.
6. On the **File to Export** page, specify the name of the file that you want to export, and then choose **Next**.
7. To close the wizard, choose **Finish** on the **Certificate Export Wizard** page, and choose **OK** in the confirmation dialog box.
8. Close **Certificates (Local Computer)**.
9. Store the file securely and ensure that you can access it from the Configuration Manager console.

   The certificate is now ready to be imported when you set up the distribution point.

> **TIP**
> You can use the same certificate file when you set up media images for an operating system deployment that does not use PXE boot, and the task sequence to install the image must contact a management point that requires HTTPS client connections.

Deploy the enrollment certificate for mobile devices

This certificate deployment has a single procedure to create and issue the enrollment certificate template on the certification authority.

Create and issue the enrollment certificate template on the certification authority

This procedure creates an enrollment certificate template for Configuration Manager mobile devices and adds it to the certification authority.

To create and issue the enrollment certificate template on the certification authority

1. Create a security group that has users who will enroll mobile devices in Configuration Manager.
2. On the member server that has Certificate Services installed, in the Certification Authority console, right-click **Certificate Templates**, and then choose **Manage** to load the Certificate Templates management console.
3. In the results pane, right-click the entry that has **Authenticated Session** in the **Template Display Name** column, and then choose **Duplicate Template**.
4. In the **Duplicate Template** dialog box, ensure that **Windows 2003 Server, Enterprise Edition** is selected, and then choose **OK**.

   > **IMPORTANT**
   > Do not select **Windows 2008 Server, Enterprise Edition**.

5. In the **Properties of New Template** dialog box, on the **General** tab, enter a template name, like

ConfigMgr Mobile Device Enrollment Certificate, to generate the enrollment certificates for the mobile devices to be managed by Configuration Manager.

6. Choose the **Subject Name** tab, make sure that **Build from this Active Directory information** is selected, select **Common name** for the **Subject name format:**, and then clear **User principal name (UPN)** from **Include this information in alternate subject name**.
7. Choose the **Security** tab, choose the security group that has users who have mobile devices to enroll, and then choose the additional permission of **Enroll**. Do not clear **Read**.
8. Choose **OK**, and then close **Certificate Templates Console**.
9. In the Certification Authority console, right-click **Certificate Templates**, choose **New**, and then choose **Certificate Template to Issue**.
10. In the **Enable Certificate Templates** dialog box, choose the new template that you just created, **ConfigMgr Mobile Device Enrollment Certificate**, and then choose **OK**.
11. If you do not need to create and issue more certificates, close the Certification Authority console.

    The mobile device enrollment certificate template is now ready to be selected when you set up a mobile device enrollment profile in the client settings.

Deploy the client certificate for Mac computers

This certificate deployment has a single procedure to create and issue the enrollment certificate template on the certification authority.

Create and issue a Mac client certificate template on the certification authority

This procedure creates a custom certificate template for Configuration Manager Mac computers and adds the certificate template to the certification authority.

> **NOTE**
>
> This procedure uses a different certificate template from the certificate template that you might have created for Windows client computers or for distribution points.
>
> When you create a new certificate template for this certificate, you can restrict the certificate request to authorized users.

To create and issue the Mac client certificate template on the certification authority

1. Create a security group that has user accounts for administrative users who will enroll the certificate on the Mac computer by using Configuration Manager.
2. On the member server that is running the Certification Authority console, right-click **Certificate Templates**, and then choose **Manage** to load the Certificate Templates management console.
3. In the results pane, right-click the entry that displays **Authenticated Session** in the **Template Display Name** column, and then choose **Duplicate Template**.
4. In the **Duplicate Template** dialog box, ensure that **Windows 2003 Server, Enterprise Edition** is selected, and then choose **OK**.

   > **IMPORTANT**
   >
   > Do not select **Windows 2008 Server, Enterprise Edition**.

5. In the **Properties of New Template** dialog box, on the **General** tab, enter a template name, like **ConfigMgr Mac Client Certificate**, to generate the Mac client certificate.

6. Choose the **Subject Name** tab, make sure that **Build from this Active Directory information** is selected, choose **Common name** for the **Subject name format:**, and then clear **User principal name (UPN)** from **Include this information in alternate subject name**.
7. Choose the **Security** tab, and then remove the **Enroll** permission from the **Domain Admins** and **Enterprise Admins** security groups.
8. Choose **Add**, specify the security group that you created in step one, and then choose **OK**.
9. Choose the **Enroll** permission for this group, and do not clear the **Read** permission.
10. Choose **OK**, and then close **Certificate Templates Console**.
11. In the Certification Authority console, right-click **Certificate Templates**, choose **New**, and then choose **Certificate Template to Issue**.
12. In the **Enable Certificate Templates** dialog box, choose the new template that you just created, **ConfigMgr Mac Client Certificate**, and then choose **OK**.
13. If you do not have to create and issue more certificates, close **Certification Authority**.

    The Mac client certificate template is now ready to be selected when you set up client settings for enrollment.

Diagnostics and usage data for Configuration Manager

7/26/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager collects diagnostics and usage data about itself, which is used by Microsoft to improve the installation experience, quality, and security of future releases.

Diagnostics and usage data is enabled for each Configuration Manager hierarchy. It consists of SQL Server queries that run on a weekly basis on each primary site and at the central administration site. When the hierarchy uses a central administration site, the data from primary sites is then replicated to that site. At the top-level site of your hierarchy, the service connection point submits this information when it checks for updates. If the service connection point is in offline mode, the information is transferred by using the service connection tool.

> **NOTE**
> Configuration Manager collects data only from the site's SQL server database, and it does not collect data directly from clients or site servers.

For more information, see the Microsoft privacy statement.

Articles

Learn more about diagnostic and usage data for Configuration Manager in the following articles:

- How diagnostics and usage data is used
- Levels of diagnostic usage data collection:
  - Diagnostic data for 1906
  - Diagnostic data for 1902
  - Diagnostic data for 1810
  - Diagnostic data for 1806
- How diagnostics and usage data is collected
- How to view diagnostics and usage data
- Frequently asked questions about diagnostics and usage data

See also

About the service connection point

How diagnostics and usage data is used for System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Diagnostic and usage data that System Center Configuration Manager collects provides Microsoft nearly immediate feedback about how the product is working and is used to adjust future updates. We are also able to see configuration data that helps us engineer and test the configurations that are in production. For example:

- The Windows server versions that are used by site servers
- The installed language packs
- The delta of the SQL schema against the product default

This data helps the engineering team plan future tests to ensure the best experience for the most common configurations. As updates to Configuration Manager are released on a faster cadence (to better support quickly moving technologies such as Windows 10 and Microsoft Intune), this data is crucial to quickly adjust and adapt.

Equally important is how the diagnostics and usage data is not used. Microsoft does not use this data for:

- Licensing audits, such as comparing customer usage against license agreements
- Auditing of products that are out of support
- Advertising based on available data such as feature usage or geolocation (time zone)

Examples of how diagnostics and usage data improves the product

Microsoft uses available data to improve to the product. Following are a few examples:

- **Revised support for older server operating systems:**

  The initial support offered by the current branch of System Center Configuration Manager limited the support timeline for Windows Server 2008 R2. After examining the usage data from customers who had upgraded to the Configuration Manager current branch, we identified the need to revise and extend this timeline to support customers who still use this server operating system to host site servers and site system roles.

- **Improved prerequisite checks:**

  Based on the usage data, we have improved the prerequisite checks for installing an update to remove obsolete rules, account for additional cases, and, in some cases, to auto-remediate some issues.

Levels of diagnostic usage data collection for version 1906

7/26/2019 • 14 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager version 1906 collects three levels of diagnostics and usage data: **Basic**, **Enhanced**, and **Full**. By default, this feature is set at the Enhanced level. The following sections provide additional detail about data collected at each level.

Changes from previous versions are noted with ***[New]***, ***[Updated]***, ***[Removed]***, or ***[Moved]***.

> **IMPORTANT**
> Configuration Manager doesn't collect site codes, sites names, IP addresses, user names, computer names, physical addresses, or email addresses on the Basic or Enhanced levels. Any collection of this information on the Full level is not purposeful. It is potentially included in advanced diagnostic information like log files or memory snapshots. Microsoft doesn't use this information to identify you, contact you, or develop advertising.

How to change the level

To change the data collection level, you need **Modify** permissions on the **Site** object class. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. Select **Hierarchy Settings** in the ribbon, and then choose the data level in the Diagnostics and Usage Data settings.

Level 1 - Basic

The Basic level includes data about your hierarchy. It's required to help improve your installation or upgrade experience. This data also helps determine the Configuration Manager updates that are applicable for your hierarchy.

For Configuration Manager version 1906, this level includes the following data:

- ***[Updated]*** Statistics about Configuration Manager console connections: OS version, language, SKU and architecture, system memory, logical processor count, connect site ID, installed .NET versions, console language packs, and capable authentication level
- Basic application and deployment type counts: total apps, total apps with multiple deployment types, total apps with dependencies, total superseded apps, and count of deployment technologies in use
- Basic Configuration Manager site hierarchy data: site list, type, version, status, client count, and time zone
- Basic database configuration: processors, memory size, memory settings, Configuration Manager database configuration, Configuration Manager database size, cluster configuration, configuration of distributed views, and change tracking version
- Basic discovery statistics: discovery count, minimum/maximum/average group sizes, and when the site is running entirely with Azure Active Directory Services
- Basic Endpoint Protection information about antimalware client versions

- Basic OS deployment counts of images
- Basic site system server information: site system roles used, internet and SSL status, OS, processors, physical or virtual machine, and usage of site server high availability
- Configuration Manager database schema (hash of all object definitions)
- Configured level for diagnostics and usage data, online or offline mode, and fast update configuration
- Count of client languages and locales
- Count of Configuration Manager client versions, OS versions, and Office versions
- Count of operating systems for managed devices and policies set by the Exchange Connector
- Count of Windows 10 devices by branch, build, and unique Active Directory forest
- Count of Windows 10 clients that use Windows Update for Business
- Database performance metrics: replication processing information, top SQL Server stored procedures by processor, and disk usage
- Distribution point and management point types and basic configuration information: protected, prestaged, PXE, multicast, SSL state, pull/peer distribution points, MDM-enabled, and SSL-enabled
- Hashed list of extensions to admin console property pages and wizards
- Setup Information:
  - Build, install type, language packs, features that you enabled
  - Pre-release use, setup media type, branch type
  - Software Assurance expiration date
  - Update pack deployment status and errors, download progress, and prerequisite errors
  - Use of update fast ring
  - Version of post-upgrade script
- SQL version, service pack level, edition, collation ID, and character set
- Diagnostics and usage data statistics: when run, runtime, errors
- Whether network discovery is enabled or disabled
- Count of clients joined to Azure Active Directory
- Count of phased deployments created by type
- Count of extended interoperability clients
- Hashed list of hardware inventory properties longer than 255 characters
- Count of clients by co-management enrollment method
- Error statistics for co-management enrollment
- Count of clients by Windows OS age, to the nearest three-month interval
- Top 10 processor names used on clients and servers
- Count and processing rates of key Configuration Manager objects: data discovery records (DDR), state messages, status messages, hardware inventory, software inventory, and overall count of files in inboxes

- Site server disk and processor performance information
- Uptime and memory usage information for Configuration Manager site server processes
- Count of crashes for Configuration Manager site server processes, and Watson signature ID, if available
- Hashed list of top SQL queries by memory usage and lock count
- Aggregated usage statistics of co-management: number of clients ever enrolled, number of enrolled clients, number of clients pending enrollment, clients receiving policy, workload states, pilot/exclusion collection sizes, and enrollment errors
- Existence of Microsoft BitLocker Administration and Monitoring (MBAM) server-side extensions
- Count of categorized and uncategorized applications for asset intelligence
- ***[New]*** Status and health of the administration service
- ***[New]*** Hash of key site attributes (site ID, SQL broker ID, and site exchange key)

Level 2 - Enhanced

The Enhanced level is the default after setup finishes. This level includes data that's collected in the Basic level and feature-specific data. It shows frequency and duration of use of different features. It also includes Configuration Manager client settings data: component name, state, and certain settings like polling intervals. Information about software updates is basic on usage, no data regarding update compliance.

Microsoft recommends this level because it provides them with the minimum data to make product and service improvements. This level doesn't collect object names (sites, users, computer, or objects), details of security-related objects, or vulnerabilities like counts of systems that require software updates.

For Configuration Manager version 1906, this level includes the following data:

Application management

- App requirements: count of built-in conditions referenced by deployment technology
- App supersedence, maximum depth of chain
- Application approval statistics and usage frequency
- Application content size statistics
- Application deployment information: use of install versus uninstall, requires approval, user interaction enabled/disabled, dependency, supersedence, and usage count of install behavior feature
- Application policy size and complexity statistics
- Available application request statistics
- Basic configuration information for packages and programs: deployment options and program flags
- Basic usage/targeting information for deployment types: user versus device targeted, required versus available, and universal apps
- Count of App-V environments and deployment properties
- Count of application applicability by OS
- Count of applications referenced in a task sequence
- Count of distinct branding for application catalog

- Count of Office 365 applications created using dashboard
- Count of packages by type
- Count of package/program deployments
- Count of Windows 10 licensed application licenses
- Count of Windows Installer deployment types by uninstall content settings
- Count of Microsoft Store for Business apps and sync statistics: summarized types of apps, licensed app status, and number of online and offline licensed apps
- Maintenance window type and duration
- Minimum/maximum/average number of application deployments per user/device per time period
- Most common application installation error codes by deployment technology
- MSI configuration options and counts
- Statistics on end-user interaction with notification for required software deployments
- Universal Data Access usage, how created
- Aggregated user device affinity statistics
- Max and average primary users per device
- Application global condition usage by type
- Software Center customization configuration
- Package Conversion Manager readiness and counts
- Count of application detection methods by type
- Count of application enforcement errors
- MSI installer properties
- Statistics of user install requests
- Aggregated statistics on the use of the email approval feature
- File count, content size, services count, and custom action count of MSIs in application catalog
- Count of devices by Office ProPlus readiness state
- ***[New]*** Aggregated statistics on the use of application groups
- ***[New]*** Aggregated statistics on Office add-ins, usage of the Office Readiness Toolkit, and counts of clients with Office 365 ProPlus

Client

- Active Management Technology (AMT) client version
- BIOS age in years
- Count of devices with Secure Boot enabled
- Count of devices by TPM state
- Client auto-upgrade: deployment configuration including client piloting and exclusion usage (extended interoperability client)

- Client cache size configuration
- Client deployment download errors
- Client health statistics and top issue summary by client version, component, OS, and workload
- Client notification operation action status: how many times each is run, max number of targeted clients, and average success rate
- Count of client installations from each source location type
- Count of client installation failures
- Count of devices virtualized by Hyper-V or Azure
- Count of Software Center actions
- Count of UEFI-enabled devices
- Deployment methods used for client and count of clients per deployment method
- List/count of enabled client agents
- OS age in months
- Number of hardware inventory classes, software inventory rules, and file collection rules
- Statistics for device health attestation: most common error codes, number of on-premises servers, and counts of devices in various states
- Count of devices by default browser
- Count of Configuration Manager-generated server authentication certificates
- Count of Microsoft Surface devices by model
- Count of client health check failures by issue type

Cloud Services

- Azure Active Directory discovery statistics
- Configuration and usage statistics of Cloud Management Gateway: counts of regions and environments, and authentication/authorization statistics
- Count of Azure Active Directory applications and services connected to Configuration Manager
- Count of collections synced to Azure Log Analytics
- Count of Upgrade Analytics Connectors
- Whether the Azure Log Analytics cloud connector is enabled
- Count of pull-distribution points with a cloud distribution point as a source location

CMPivot

- CMPivot usage statistics
- Count of saved CMPivot queries
- Count of queries by entity type

Co-management

- Enrollment schedule and historical statistics

- Count of clients eligible for co-management
- Associated Microsoft Intune tenant

Collections

- Collection ID usage (not running out of IDs)
- Collection evaluation statistics: query time, assigned versus unassigned counts, counts by type, ID rollover, and rule usage
- Collections without a deployment
- ***[New]*** Count of collections synchronized to Azure Active Directory

Compliance settings

- Basic configuration baseline information: count, number of deployments, and number of references
- Compliance policy error statistics
- Count of configuration items by type
- Count of deployments that reference built-in settings, including remediate setting
- Count of rules and deployments created for custom settings, including remediate setting
- Count of deployed Simple Certificate Enrollment Protocol (SCEP), VPN, Wi-Fi, certificate (.pfx), and compliance policy templates
- Count of SCEP certificate, VPN, Wi-Fi, certificate (.pfx), and compliance policy deployments by platform
- Windows Hello for Business policy (created, deployed)
- Count of deployed Microsoft Edge browser policies
- Count of OneDrive policies (created, deployed)

Content

- Boundary group statistics: how many fast, how many slow, count per group, and fallback relationships
- Boundary group information: count of boundaries and site systems that are assigned to each boundary group
- Boundary group relationships and fallback configuration
- Client content download statistics
- Count of boundaries by type
- Count of peer cache clients, usage statistic, and partial download statistics
- Distribution Manager configuration information: threads, retry delay, number of retries, and pull distribution point settings
- Distribution point configuration information: use of branch cache and distribution point monitoring
- Distribution point group information: count of packages and distribution points that are assigned to each distribution point group
- Content library type, whether local or remote
- Count of boundary groups by configuration

Endpoint Protection

- Microsoft Defender Advanced Threat Protection (ATP) policies (formerly known as Windows Defender ATP): count of policies, and whether policies are deployed.
- Count of alerts that are configured for Endpoint Protection feature
- Count of collections that are selected to appear in Endpoint Protection dashboard
- Count of Windows Defender Exploit Guard policies, deployments, and targeted clients
- Endpoint Protection deployment errors, count of Endpoint Protection policy deployment error codes
- Endpoint Protection antimalware and Windows Firewall policy usage (number of unique policies assigned to group). This data doesn't include any information about the settings included in the policy.

Migration

- Count of migrated objects (use of migration wizard)

Mobile device management (MDM)

- Count of issued mobile device actions: lock, pin rest, wipe, retire, and sync now commands
- Count of mobile device policies
- Count of mobile devices Configuration Manager and Microsoft Intune manages, and how you enrolled them (bulk, user-based)
- Count of users who have multiple enrolled mobile devices
- Mobile device polling schedule and statistics for mobile device check-in duration

Microsoft Intune troubleshooting

- Count and size of device actions (wipe, retire, lock), usage data, and data messages that are replicated to Microsoft Intune
- Count and size of state, status, inventory, RDR, DDR, UDX, Tenant state, POL, LOG, Cert, CRP, Resync, CFD, RDO, BEX, ISM, and compliance messages that are downloaded from Microsoft Intune
- Full and delta user synchronization statistics for Microsoft Intune

On-premises mobile device management (MDM)

- Count of Windows 10 bulk enrollment packages and profiles
- Deployment success/failure statistics for on-premises MDM application deployments

OS deployment

- Count of boot images, drivers, driver packages, multicast-enabled distribution points, PXE-enabled distribution points, and task sequences
- Count of boot images by Configuration Manager client version
- Count of boot images by Windows PE version
- Count of edition upgrade policies
- Count of hardware identifiers excluded from PXE
- Count of OS deployment by OS version
- Count of OS upgrades over time
- Count of task sequence deployments using option to pre-download content
- Counts of task sequence step usage

- Version of Windows ADK installed
- Count of image servicing tasks
- Count of imported machines
- ***[New]*** Count of duplicate hardware identifiers (MAC address and SMBIOS GUID) excluded from PXE and client registration
- ***[New]*** Count of task sequences by type (OS deployment or generic task sequence)
- ***[New]*** Count of packages with pre-cache content settings

Site updates

- Versions of installed Configuration Manager hotfixes

Software Updates

- Available and deadline deltas that are used in automatic deployment rules
- Average and maximum number of assignments per update
- Client update evaluation and scan schedules
- Classifications synced by the software update point
- Cluster patching statistics
- Configuration of Windows 10 express updates
- Configurations that are used for active Windows 10 servicing plans
- Count of deployed Office 365 updates
- Count of Microsoft Surface drivers synced
- Count of update groups and assignments
- Count of update packages and the maximum/minimum/average number of distribution points that are targeted with packages
- Count of updates that are created and deployed with System Center Update Publisher
- Count of Windows Update for Business policies created and deployed
- Aggregated statistics of Windows Update for Business configurations
- Number of automatic deployment rules that are tied to synchronization
- Number of automatic deployment rules that create new or add updates to an existing group
- Number of automatic deployment rules that have multiple deployments
- Number of update groups and minimum/maximum/average number of updates per group
- Number of updates and percentage of updates that are deployed, expired, superseded, downloaded, and contain EULAs
- Software update point load-balancing statistics
- Software update point synchronization schedule
- Total/average number of collections that have software update deployments and the maximum/average number of deployed updates

- Update scan error codes and machine count
- Windows 10 dashboard content versions
- Count of third-party software update catalog subscriptions and usage
- Count of software updates deployed with and without content
- Aggregated statistics on the number of UUP updates that are required, deployed, expired, superseded, and downloaded
- Use of UUP product categories
- Count of clients that have deployed at least one UUP quality update or UUP feature update
- Top UUP error codes and count of affected devices
- ***[New]*** List of subscriptions to third-party software update catalogs
- ***[New]*** Use of WSUS maintenance settings

SQL/performance data

- Configuration and duration of site summarization
- Count of largest database tables
- Discovery operational statistics (count of objects found)
- Discovery types, enabled, and schedule (full, incremental)
- SQL AlwaysOn replica information, usage, and health status
- SQL change tracking performance issues, retention period, and autocleanup state
- SQL change tracking retention period
- State and status message performance statistics including most common and most expensive message types
- Management point traffic statistics (total bytes sent and received by endpoint)
- Management point performance counter measurements
- ***[New]*** Aggregated performance statistics of calls made to Software Center endpoints on the management point

Miscellaneous

- Configuration of data warehouse service point including synchronization schedule, average time, and use of customized tables feature
- Count of scripts and run/edit statistics
- Count of sites with Wake On LAN (WOL)
- Reporting usage and performance statistics
- Phased deployment usage statistics
- Management insights item counts and progress
- Count of crashes for unique non-Configuration Manager processes on the site server, and Watson signature ID, if available
- Aggregated statistics on Desktop Analytics enrollment errors and usage

- Count of non-critical console notifications
- Aggregated system boot time statistics by OS, form-factor, and drive type
- ***[New]*** Aggregated statistics on the use of Desktop Analytics
- ***[New]*** SQL maintenance task configuration and status

Level 3 - Full

The Full level includes all data in the Basic and Enhanced levels. It also includes additional information about Endpoint Protection, update compliance percentages, and software update information. This level can also include advanced diagnostic information like system files and memory snapshots. This advanced data might include personal information exists in memory or log files at the time of capture.

For Configuration Manager version 1906, this level includes the following data:

- Automatic deployment rule evaluation schedule information
- ATP health summary
- Collection evaluation and refresh statistics
- Compliance policy statistics on compliance and errors
- Compliance settings: SCEP, VPN, Wi-Fi, and compliance policy template configuration details
- DCM config pack for Configuration Manager usage
- Detailed client deployment installation errors
- Endpoint Protection health summary: including count of protected, at risk, unknown, and unsupported clients
- Endpoint Protection policy configuration
- List of processes configured with installation behavior for applications
- Minimum/maximum/average number of hours since last software update scan
- Minimum/maximum/average number of inactive clients in software update deployment collections
- Minimum/maximum/average number of software updates per package
- MSI product code deployment statistics
- Overall compliance of software update deployments
- Count of groups that have expired software updates
- Software update deployment error codes and counts
- Software update deployment information: percentage of deployments that are targeted with client versus UTC time, required versus optional versus silent, and reboot suppression
- Software update products synced by software update point
- Software update scan success percentages
- Top 50 CPUs in the environment
- Type of Exchange Active Sync (EAS) conditional access policies (block or quarantine) for devices that Microsoft Intune manages

- Microsoft Store for Business application details: non-aggregate list of synced applications including AppID, online state or offline state, and total purchased license counts
- Count of clients pushed with option to not allow fallback to NTLM
- ***[New]*** List of Configuration Manager console extensions

Levels of diagnostic usage data collection for version 1902

7/9/2019 • 14 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager version 1902 collects three levels of diagnostics and usage data: **Basic**, **Enhanced**, and **Full**. By default, this feature is set at the Enhanced level. The following sections provide additional detail about data collected at each level.

Changes from previous versions are noted with ***[New]***, ***[Updated]***, ***[Removed]***, or ***[Moved]***.

> **IMPORTANT**
> Configuration Manager doesn't collect site codes, sites names, IP addresses, user names, computer names, physical addresses, or email addresses on the Basic or Enhanced levels. Any collection of this information on the Full level is not purposeful. It is potentially included in advanced diagnostic information like log files or memory snapshots. Microsoft doesn't use this information to identify you, contact you, or develop advertising.

How to change the level

To change the data collection level, you need **Modify** permissions on the **Site** object class. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. Select **Hierarchy Settings** in the ribbon, and then choose the data level in the Diagnostics and Usage Data settings.

Level 1 - Basic

The Basic level includes data about your hierarchy. It's required to help improve your installation or upgrade experience. This data also helps determine the Configuration Manager updates that are applicable for your hierarchy.

For Configuration Manager version 1902, this level includes the following data:

- Statistics about Configuration Manager console connections: OS version, language, SKU and architecture, system memory, logical processor count, connect site ID, installed .NET versions, and console language packs
- Basic application and deployment type counts: total apps, total apps with multiple deployment types, total apps with dependencies, total superseded apps, and count of deployment technologies in use
- Basic Configuration Manager site hierarchy data: site list, type, version, status, client count, and time zone
- Basic database configuration: processors, memory size, memory settings, Configuration Manager database configuration, Configuration Manager database size, cluster configuration, configuration of distributed views, and change tracking version
- Basic discovery statistics: discovery count, minimum/maximum/average group sizes, and when the site is running entirely with Azure Active Directory Services
- Basic Endpoint Protection information about antimalware client versions

- Basic OS deployment counts of images
- Basic site system server information: site system roles used, internet and SSL status, OS, processors, physical or virtual machine, and usage of site server high availability
- Configuration Manager database schema (hash of all object definitions)
- Configured level for diagnostics and usage data, online or offline mode, and fast update configuration
- Count of client languages and locales
- Count of Configuration Manager client versions, OS versions, and Office versions
- Count of operating systems for managed devices and policies set by the Exchange Connector
- Count of Windows 10 devices by branch, build, and unique Active Directory forest
- Count of Windows 10 clients that use Windows Update for Business
- Database performance metrics: replication processing information, top SQL Server stored procedures by processor, and disk usage
- Distribution point and management point types and basic configuration information: protected, prestaged, PXE, multicast, SSL state, pull/peer distribution points, MDM-enabled, and SSL-enabled
- Hashed list of extensions to admin console property pages and wizards
- Setup Information:
  - Build, install type, language packs, features that you enabled
  - Pre-release use, setup media type, branch type
  - Software Assurance expiration date
  - Update pack deployment status and errors, download progress, and prerequisite errors
  - Use of update fast ring
  - Version of post-upgrade script
- SQL version, service pack level, edition, collation ID, and character set
- Diagnostics and usage data statistics: when run, runtime, errors
- Whether network discovery is enabled or disabled
- Count of clients joined to Azure Active Directory
- Count of phased deployments created by type
- Count of extended interoperability clients
- Hashed list of hardware inventory properties longer than 255 characters
- Count of clients by co-management enrollment method
- Error statistics for co-management enrollment
- Count of clients by Windows OS age, to the nearest three-month interval
- Top 10 processor names used on clients and servers
- Count and processing rates of key Configuration Manager objects: data discovery records (DDR), state messages, status messages, hardware inventory, software inventory, and overall count of files in inboxes

- Site server disk and processor performance information
- Uptime and memory usage information for Configuration Manager site server processes
- Count of crashes for Configuration Manager site server processes, and Watson signature ID, if available
- Hashed list of top SQL queries by memory usage and lock count
- Aggregated usage statistics of co-management: number of clients ever enrolled, number of enrolled clients, number of clients pending enrollment, clients receiving policy, workload states, pilot/exclusion collection sizes, and enrollment errors
- ***[New]*** Existence of Microsoft BitLocker Administration and Monitoring (MBAM) server-side extensions
- ***[New]*** Count of categorized and uncategorized applications for asset intelligence

Level 2 - Enhanced

The Enhanced level is the default after setup finishes. This level includes data that's collected in the Basic level and feature-specific data. It shows frequency and duration of use of different features. It also includes Configuration Manager client settings data: component name, state, and certain settings like polling intervals. Information about software updates is basic on usage, no data regarding update compliance.

Microsoft recommends this level because it provides them with the minimum data to make product and service improvements. This level doesn't collect object names (sites, users, computer, or objects), details of security-related objects, or vulnerabilities like counts of systems that require software updates.

For Configuration Manager version 1902, this level includes the following data:

Application management

- App requirements: count of built-in conditions referenced by deployment technology
- App supersedence, maximum depth of chain
- Application approval statistics and usage frequency
- Application content size statistics
- Application deployment information: use of install versus uninstall, requires approval, user interaction enabled/disabled, dependency, supersedence, and usage count of install behavior feature
- Application policy size and complexity statistics
- Available application request statistics
- Basic configuration information for packages and programs: deployment options and program flags
- Basic usage/targeting information for deployment types: user versus device targeted, required versus available, and universal apps
- Count of App-V environments and deployment properties
- Count of application applicability by OS
- Count of applications referenced in a task sequence
- Count of distinct branding for application catalog
- Count of Office 365 applications created using dashboard
- Count of packages by type

- Count of package/program deployments
- Count of Windows 10 licensed application licenses
- Count of Windows Installer deployment types by uninstall content settings
- Count of Microsoft Store for Business apps and sync statistics: summarized types of apps, licensed app status, and number of online and offline licensed apps
- Maintenance window type and duration
- Minimum/maximum/average number of application deployments per user/device per time period
- Most common application installation error codes by deployment technology
- MSI configuration options and counts
- Statistics on end-user interaction with notification for required software deployments
- Universal Data Access usage, how created
- Aggregated user device affinity statistics
- Max and average primary users per device
- Application global condition usage by type
- Software Center customization configuration
- Package Conversion Manager readiness and counts
- Count of application detection methods by type
- Count of application enforcement errors
- MSI installer properties
- Statistics of user install requests
- Aggregated statistics on the use of the email approval feature
- File count, content size, services count, and custom action count of MSIs in application catalog
- ***[New]*** Count of devices by Office ProPlus readiness state

Client

- Active Management Technology (AMT) client version
- BIOS age in years
- Count of devices with Secure Boot enabled
- Count of devices by TPM state
- Client auto-upgrade: deployment configuration including client piloting and exclusion usage (extended interoperability client)
- Client cache size configuration
- Client deployment download errors
- ***[Updated]*** Client health statistics and top issue summary by client version, component, OS, and workload
- Client notification operation action status: how many times each is run, max number of targeted clients, and average success rate

- Count of client installations from each source location type
- Count of client installation failures
- Count of devices virtualized by Hyper-V or Azure
- Count of Software Center actions
- Count of UEFI-enabled devices
- Deployment methods used for client and count of clients per deployment method
- List/count of enabled client agents
- OS age in months
- Number of hardware inventory classes, software inventory rules, and file collection rules
- Statistics for device health attestation: most common error codes, number of on-premises servers, and counts of devices in various states
- Count of devices by default browser
- Count of Configuration Manager-generated server authentication certificates
- Count of Microsoft Surface devices by model
- ***[New]*** Count of client health check failures by issue type

Cloud Services

- Azure Active Directory discovery statistics
- Configuration and usage statistics of Cloud Management Gateway: counts of regions and environments, and authentication/authorization statistics
- Count of Azure Active Directory applications and services connected to Configuration Manager
- Count of collections synced to Azure Log Analytics
- Count of Upgrade Analytics Connectors
- Whether the Azure Log Analytics cloud connector is enabled
- Count of pull-distribution points with a cloud distribution point as a source location

CMPivot

- CMPivot usage statistics
- Count of saved CMPivot queries
- Count of queries by entity type

Co-management

- Enrollment schedule and historical statistics
- Count of clients eligible for co-management
- Associated Microsoft Intune tenant

Collections

- Collection ID usage (not running out of IDs)
- Collection evaluation statistics: query time, assigned versus unassigned counts, counts by type, ID rollover,

and rule usage

- Collections without a deployment

Compliance settings

- Basic configuration baseline information: count, number of deployments, and number of references
- Compliance policy error statistics
- Count of configuration items by type
- Count of deployments that reference built-in settings, including remediate setting
- Count of rules and deployments created for custom settings, including remediate setting
- Count of deployed Simple Certificate Enrollment Protocol (SCEP), VPN, Wi-Fi, certificate (.pfx), and compliance policy templates
- Count of SCEP certificate, VPN, Wi-Fi, certificate (.pfx), and compliance policy deployments by platform
- Windows Hello for Business policy (created, deployed)
- Count of deployed Microsoft Edge browser policies
- ***[New]*** Count of OneDrive policies (created, deployed)

Content

- Boundary group statistics: how many fast, how many slow, count per group, and fallback relationships
- Boundary group information: count of boundaries and site systems that are assigned to each boundary group
- Boundary group relationships and fallback configuration
- Client content download statistics
- Count of boundaries by type
- Count of peer cache clients, usage statistic, and partial download statistics
- Distribution Manager configuration information: threads, retry delay, number of retries, and pull distribution point settings
- Distribution point configuration information: use of branch cache and distribution point monitoring
- Distribution point group information: count of packages and distribution points that are assigned to each distribution point group
- Content library type, whether local or remote
- Count of boundary groups by configuration

Endpoint Protection

- Microsoft Defender Advanced Threat Protection (ATP) policies (formerly known as Windows Defender ATP): count of policies, and whether policies are deployed.
- Count of alerts that are configured for Endpoint Protection feature
- Count of collections that are selected to appear in Endpoint Protection dashboard
- Count of Windows Defender Exploit Guard policies, deployments, and targeted clients
- Endpoint Protection deployment errors, count of Endpoint Protection policy deployment error codes

- Endpoint Protection antimalware and Windows Firewall policy usage (number of unique policies assigned to group). This data doesn't include any information about the settings included in the policy.

Migration

- Count of migrated objects (use of migration wizard)

Mobile device management (MDM)

- Count of issued mobile device actions: lock, pin rest, wipe, retire, and sync now commands
- Count of mobile device policies
- Count of mobile devices Configuration Manager and Microsoft Intune manages, and how you enrolled them (bulk, user-based)
- Count of users who have multiple enrolled mobile devices
- Mobile device polling schedule and statistics for mobile device check-in duration

Microsoft Intune troubleshooting

- Count and size of device actions (wipe, retire, lock), usage data, and data messages that are replicated to Microsoft Intune
- Count and size of state, status, inventory, RDR, DDR, UDX, Tenant state, POL, LOG, Cert, CRP, Resync, CFD, RDO, BEX, ISM, and compliance messages that are downloaded from Microsoft Intune
- Full and delta user synchronization statistics for Microsoft Intune

On-premises mobile device management (MDM)

- Count of Windows 10 bulk enrollment packages and profiles
- Deployment success/failure statistics for on-premises MDM application deployments

OS deployment

- Count of boot images, drivers, driver packages, multicast-enabled distribution points, PXE-enabled distribution points, and task sequences
- Count of boot images by Configuration Manager client version
- Count of boot images by Windows PE version
- Count of edition upgrade policies
- Count of hardware identifiers excluded from PXE
- Count of OS deployment by OS version
- Count of OS upgrades over time
- Count of task sequence deployments using option to pre-download content
- Counts of task sequence step usage
- Version of Windows ADK installed
- Count of image servicing tasks
- Count of imported machines

Site updates

- Versions of installed Configuration Manager hotfixes

Software Updates

- Available and deadline deltas that are used in automatic deployment rules
- Average and maximum number of assignments per update
- Client update evaluation and scan schedules
- Classifications synced by the software update point
- Cluster patching statistics
- Configuration of Windows 10 express updates
- Configurations that are used for active Windows 10 servicing plans
- Count of deployed Office 365 updates
- Count of Microsoft Surface drivers synced
- Count of update groups and assignments
- Count of update packages and the maximum/minimum/average number of distribution points that are targeted with packages
- Count of updates that are created and deployed with System Center Update Publisher
- Count of Windows Update for Business policies created and deployed
- Aggregated statistics of Windows Update for Business configurations
- Number of automatic deployment rules that are tied to synchronization
- Number of automatic deployment rules that create new or add updates to an existing group
- Number of automatic deployment rules that have multiple deployments
- Number of update groups and minimum/maximum/average number of updates per group
- Number of updates and percentage of updates that are deployed, expired, superseded, downloaded, and contain EULAs
- Software update point load-balancing statistics
- Software update point synchronization schedule
- Total/average number of collections that have software update deployments and the maximum/average number of deployed updates
- Update scan error codes and machine count
- Windows 10 dashboard content versions
- Count of third-party software update catalog subscriptions and usage
- Count of software updates deployed with and without content
- Aggregated statistics on the number of UUP updates that are required, deployed, expired, superseded, and downloaded
- Use of UUP product categories
- Count of clients that have deployed at least one UUP quality update or UUP feature update
- Top UUP error codes and count of affected devices

SQL/performance data

- Configuration and duration of site summarization
- Count of largest database tables
- Discovery operational statistics (count of objects found)
- Discovery types, enabled, and schedule (full, incremental)
- SQL AlwaysOn replica information, usage, and health status
- SQL change tracking performance issues, retention period, and autocleanup state
- SQL change tracking retention period
- State and status message performance statistics including most common and most expensive message types
- Management point traffic statistics (total bytes sent and received by endpoint)
- Management point performance counter measurements

Miscellaneous

- ***[Updated]*** Configuration of data warehouse service point including synchronization schedule, average time, and use of customized tables feature
- ***[Updated]*** Count of scripts and run/edit statistics
- Count of sites with Wake On LAN (WOL)
- Reporting usage and performance statistics
- Phased deployment usage statistics
- Management insights item counts and progress
- Count of crashes for unique non-Configuration Manager processes on the site server, and Watson signature ID, if available
- ***[New]*** Aggregated statistics on Desktop Analytics enrollment errors and usage
- ***[New]*** Count of non-critical console notifications
- ***[New]*** Aggregated system boot time statistics by OS, form-factor, and drive type

Level 3 - Full

The Full level includes all data in the Basic and Enhanced levels. It also includes additional information about Endpoint Protection, update compliance percentages, and software update information. This level can also include advanced diagnostic information like system files and memory snapshots. This advanced data might include personal information exists in memory or log files at the time of capture.

For Configuration Manager version 1902, this level includes the following data:

- Automatic deployment rule evaluation schedule information
- ATP health summary
- Collection evaluation and refresh statistics
- Compliance policy statistics on compliance and errors
- Compliance settings: SCEP, VPN, Wi-Fi, and compliance policy template configuration details

- DCM config pack for Configuration Manager usage
- Detailed client deployment installation errors
- Endpoint Protection health summary: including count of protected, at risk, unknown, and unsupported clients
- Endpoint Protection policy configuration
- List of processes configured with installation behavior for applications
- Minimum/maximum/average number of hours since last software update scan
- Minimum/maximum/average number of inactive clients in software update deployment collections
- Minimum/maximum/average number of software updates per package
- MSI product code deployment statistics
- Overall compliance of software update deployments
- Count of groups that have expired software updates
- Software update deployment error codes and counts
- Software update deployment information: percentage of deployments that are targeted with client versus UTC time, required versus optional versus silent, and reboot suppression
- Software update products synced by software update point
- Software update scan success percentages
- Top 50 CPUs in the environment
- Type of Exchange Active Sync (EAS) conditional access policies (block or quarantine) for devices that Microsoft Intune manages
- Microsoft Store for Business application details: non-aggregate list of synced applications including AppID, online state or offline state, and total purchased license counts
- Count of clients pushed with option to not allow fallback to NTLM

Levels of diagnostic usage data collection for version 1810

7/9/2019 • 13 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager version 1810 collects three levels of diagnostics and usage data: **Basic**, **Enhanced**, and **Full**. By default, this feature is set at the Enhanced level. The following sections provide additional detail about data collected at each level.

Changes from previous versions are noted with ***[New]***, ***[Updated]***, ***[Removed]***, or ***[Moved]***.

> **IMPORTANT**
> Configuration Manager doesn't collect site codes, sites names, IP addresses, user names, computer names, physical addresses, or email addresses on the Basic or Enhanced levels. Any collection of this information on the Full level is not purposeful. It is potentially included in advanced diagnostic information like log files or memory snapshots. Microsoft doesn't use this information to identify you, contact you, or develop advertising.

How to change the level

To change the data collection level, you need **Modify** permissions on the **Site** object class. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. Select **Hierarchy Settings** in the ribbon, and then choose the data level in the Diagnostics and Usage Data settings.

Level 1 - Basic

The Basic level includes data about your hierarchy. It's required to help improve your installation or upgrade experience. This data also helps determine the Configuration Manager updates that are applicable for your hierarchy.

For Configuration Manager version 1810, this level includes the following data:

- Statistics about Configuration Manager console connections: OS version, language, SKU and architecture, system memory, logical processor count, connect site ID, installed .NET versions, and console language packs
- Basic application and deployment type counts: total apps, total apps with multiple deployment types, total apps with dependencies, total superseded apps, and count of deployment technologies in use
- Basic Configuration Manager site hierarchy data: site list, type, version, status, client count, and time zone
- ***[Updated]*** Basic database configuration: processors, memory size, memory settings, Configuration Manager database configuration, Configuration Manager database size, cluster configuration, configuration of distributed views, and change tracking version
- Basic discovery statistics: discovery count, minimum/maximum/average group sizes, and when the site is running entirely with Azure Active Directory Services
- Basic Endpoint Protection information about antimalware client versions

- Basic OS deployment counts of images
- Basic site system server information: site system roles used, internet and SSL status, OS, processors, physical or virtual machine, and usage of site server high availability
- Configuration Manager database schema (hash of all object definitions)
- Configured level for diagnostics and usage data, online or offline mode, and fast update configuration
- Count of client languages and locales
- Count of Configuration Manager client versions, OS versions, and Office versions
- Count of operating systems for managed devices and policies set by the Exchange Connector
- ***[Updated]*** Count of Windows 10 devices by branch, build, and unique Active Directory forest
- Count of Windows 10 clients that use Windows Update for Business
- Database performance metrics: replication processing information, top SQL Server stored procedures by processor, and disk usage
- Distribution point and management point types and basic configuration information: protected, prestaged, PXE, multicast, SSL state, pull/peer distribution points, MDM-enabled, and SSL-enabled
- Hashed list of extensions to admin console property pages and wizards
- Setup Information:
  - Build, install type, language packs, features that you enabled
  - Pre-release use, setup media type, branch type
  - Software Assurance expiration date
  - Update pack deployment status and errors, download progress, and prerequisite errors
  - Use of update fast ring
  - Version of post-upgrade script
- SQL version, service pack level, edition, collation ID, and character set
- Diagnostics and usage data statistics: when run, runtime, errors
- Whether network discovery is enabled or disabled
- Count of clients joined to Azure Active Directory
- Count of phased deployments created by type
- Count of extended interoperability clients
- Hashed list of hardware inventory properties longer than 255 characters
- Count of clients by co-management enrollment method
- Error statistics for co-management enrollment
- Count of clients by Windows OS age, to the nearest three-month interval
- ***[Updated]*** Top 10 processor names used on clients and servers
- Count and processing rates of key Configuration Manager objects: data discovery records (DDR), state messages, status messages, hardware inventory, software inventory, and overall count of files in inboxes

- Site server disk and processor performance information
- Uptime and memory usage information for Configuration Manager site server processes
- Count of crashes for Configuration Manager site server processes, and Watson signature ID, if available
- ***[New]*** Hashed list of top SQL queries by memory usage and lock count
- ***[Moved, updated]*** Aggregated usage statistics of co-management: number of clients ever enrolled, number of enrolled clients, number of clients pending enrollment, clients receiving policy, workload states, pilot/exclusion collection sizes, and enrollment errors

Level 2 - Enhanced

The Enhanced level is the default after setup finishes. This level includes data that's collected in the Basic level and feature-specific data. It shows frequency and duration of use of different features. It also includes Configuration Manager client settings data: component name, state, and certain settings like polling intervals. Information about software updates is basic on usage, no data regarding update compliance.

Microsoft recommends this level because it provides them with the minimum data to make product and service improvements. This level doesn't collect object names (sites, users, computer, or objects), details of security-related objects, or vulnerabilities like counts of systems that require software updates.

For Configuration Manager version 1810, this level includes the following data:

Application management

- App requirements: count of built-in conditions referenced by deployment technology
- App supersedence, maximum depth of chain
- Application approval statistics and usage frequency
- Application content size statistics
- Application deployment information: use of install versus uninstall, requires approval, user interaction enabled/disabled, dependency, supersedence, and usage count of install behavior feature
- Application policy size and complexity statistics
- Available application request statistics
- Basic configuration information for packages and programs: deployment options and program flags
- Basic usage/targeting information for deployment types: user versus device targeted, required versus available, and universal apps
- Count of App-V environments and deployment properties
- Count of application applicability by OS
- Count of applications referenced in a task sequence
- Count of distinct branding for application catalog
- Count of Office 365 applications created using dashboard
- Count of packages by type
- Count of package/program deployments
- Count of Windows 10 licensed application licenses

- Count of Windows Installer deployment types by uninstall content settings
- Count of Microsoft Store for Business apps and sync statistics: summarized types of apps, licensed app status, and number of online and offline licensed apps
- Maintenance window type and duration
- Minimum/maximum/average number of application deployments per user/device per time period
- Most common application installation error codes by deployment technology
- MSI configuration options and counts
- Statistics on end-user interaction with notification for required software deployments
- Universal Data Access usage, how created
- Aggregated user device affinity statistics
- Max and average primary users per device
- Application global condition usage by type
- Software Center customization configuration
- Package Conversion Manager readiness and counts
- Count of application detection methods by type
- Count of application enforcement errors
- MSI installer properties
- Statistics of user install requests
- ***[New]*** Aggregated statistics on the use of the email approval feature
- ***[New]*** File count, content size, services count, and custom action count of MSIs in application catalog

Client

- Active Management Technology (AMT) client version
- BIOS age in years
- Count of devices with Secure Boot enabled
- Count of devices by TPM state
- Client auto-upgrade: deployment configuration including client piloting and exclusion usage (extended interoperability client)
- Client cache size configuration
- Client deployment download errors
- Client health statistics and top issue summary by client version
- Client notification operation action status: how many times each is run, max number of targeted clients, and average success rate
- Count of client installations from each source location type
- Count of client installation failures
- Count of devices virtualized by Hyper-V or Azure

- Count of Software Center actions
- Count of UEFI-enabled devices
- Deployment methods used for client and count of clients per deployment method
- List/count of enabled client agents
- OS age in months
- Number of hardware inventory classes, software inventory rules, and file collection rules
- Statistics for device health attestation: most common error codes, number of on-premises servers, and counts of devices in various states
- Count of devices by default browser
- Count of Configuration Manager-generated server authentication certificates
- Count of Microsoft Surface devices by model

Cloud Services

- Azure Active Directory discovery statistics
- Configuration and usage statistics of Cloud Management Gateway: counts of regions and environments, and authentication/authorization statistics
- Count of Azure Active Directory applications and services connected to Configuration Manager
- Count of collections synced to Azure Log Analytics
- Count of Upgrade Analytics Connectors
- Whether the Azure Log Analytics cloud connector is enabled
- Count of pull-distribution points with a cloud distribution point as a source location

CMPivot

- CMPivot usage statistics
- ***[New]*** Count of saved CMPivot queries
- ***[New]*** Count of queries by entity type

Co-management

- Enrollment schedule and historical statistics
- Count of clients eligible for co-management
- Associated Microsoft Intune tenant

Collections

- Collection ID usage (not running out of IDs)
- Collection evaluation statistics: query time, assigned versus unassigned counts, counts by type, ID rollover, and rule usage
- Collections without a deployment

Compliance settings

- Basic configuration baseline information: count, number of deployments, and number of references
- Compliance policy error statistics

- Count of configuration items by type
- Count of deployments that reference built-in settings, including remediate setting
- Count of rules and deployments created for custom settings, including remediate setting
- Count of deployed Simple Certificate Enrollment Protocol (SCEP), VPN, Wi-Fi, certificate (.pfx), and compliance policy templates
- Count of SCEP certificate, VPN, Wi-Fi, certificate (.pfx), and compliance policy deployments by platform
- Windows Hello for Business policy (created, deployed)
- Count of deployed Microsoft Edge browser policies

Content

- Boundary group statistics: how many fast, how many slow, count per group, and fallback relationships
- Boundary group information: count of boundaries and site systems that are assigned to each boundary group
- Boundary group relationships and fallback configuration
- Client content download statistics
- Count of boundaries by type
- Count of peer cache clients, usage statistic, and partial download statistics
- Distribution Manager configuration information: threads, retry delay, number of retries, and pull distribution point settings
- Distribution point configuration information: use of branch cache and distribution point monitoring
- Distribution point group information: count of packages and distribution points that are assigned to each distribution point group
- Content library type, whether local or remote
- ***[New]*** Count of boundary groups by configuration

Endpoint Protection

- Microsoft Defender Advanced Threat Protection (ATP) policies (formerly known as Windows Defender ATP): count of policies, and whether policies are deployed.
- Count of alerts that are configured for Endpoint Protection feature
- Count of collections that are selected to appear in Endpoint Protection dashboard
- Count of Windows Defender Exploit Guard policies, deployments, and targeted clients
- Endpoint Protection deployment errors, count of Endpoint Protection policy deployment error codes
- Endpoint Protection antimalware and Windows Firewall policy usage (number of unique policies assigned to group). This data doesn't include any information about the settings included in the policy.

Migration

- Count of migrated objects (use of migration wizard)

Mobile device management (MDM)

- Count of issued mobile device actions: lock, pin rest, wipe, retire, and sync now commands
- Count of mobile device policies

- Count of mobile devices Configuration Manager and Microsoft Intune manages, and how you enrolled them (bulk, user-based)
- Count of users who have multiple enrolled mobile devices
- Mobile device polling schedule and statistics for mobile device check-in duration

Microsoft Intune troubleshooting

- Count and size of device actions (wipe, retire, lock), usage data, and data messages that are replicated to Microsoft Intune
- Count and size of state, status, inventory, RDR, DDR, UDX, Tenant state, POL, LOG, Cert, CRP, Resync, CFD, RDO, BEX, ISM, and compliance messages that are downloaded from Microsoft Intune
- Full and delta user synchronization statistics for Microsoft Intune

On-premises mobile device management (MDM)

- Count of Windows 10 bulk enrollment packages and profiles
- Deployment success/failure statistics for on-premises MDM application deployments

OS deployment

- Count of boot images, drivers, driver packages, multicast-enabled distribution points, PXE-enabled distribution points, and task sequences
- Count of boot images by Configuration Manager client version
- Count of boot images by Windows PE version
- Count of edition upgrade policies
- Count of hardware identifiers excluded from PXE
- Count of OS deployment by OS version
- Count of OS upgrades over time
- Count of task sequence deployments using option to pre-download content
- Counts of task sequence step usage
- Version of Windows ADK installed
- Count of image servicing tasks
- ***[New]*** Count of imported machines

Site updates

- Versions of installed Configuration Manager hotfixes

Software Updates

- Available and deadline deltas that are used in automatic deployment rules
- Average and maximum number of assignments per update
- Client update evaluation and scan schedules
- Classifications synced by the software update point
- Cluster patching statistics
- Configuration of Windows 10 express updates

- Configurations that are used for active Windows 10 servicing plans
- Count of deployed Office 365 updates
- Count of Microsoft Surface drivers synced
- Count of update groups and assignments
- Count of update packages and the maximum/minimum/average number of distribution points that are targeted with packages
- Count of updates that are created and deployed with System Center Update Publisher
- Count of Windows Update for Business policies created and deployed
- Aggregated statistics of Windows Update for Business configurations
- Number of automatic deployment rules that are tied to synchronization
- Number of automatic deployment rules that create new or add updates to an existing group
- Number of automatic deployment rules that have multiple deployments
- Number of update groups and minimum/maximum/average number of updates per group
- Number of updates and percentage of updates that are deployed, expired, superseded, downloaded, and contain EULAs
- Software update point load-balancing statistics
- Software update point synchronization schedule
- Total/average number of collections that have software update deployments and the maximum/average number of deployed updates
- Update scan error codes and machine count
- Windows 10 dashboard content versions
- Count of third-party software update catalog subscriptions and usage
- Count of software updates deployed with and without content
- ***[New]*** Aggregated statistics on the number of UUP updates that are required, deployed, expired, superseded, and downloaded
- ***[New]*** Use of UUP product categories
- ***[New]*** Count of clients that have deployed at least one UUP quality update or UUP feature update
- ***[New]*** Top UUP error codes and count of affected devices

SQL/performance data

- Configuration and duration of site summarization
- Count of largest database tables
- Discovery operational statistics (count of objects found)
- Discovery types, enabled, and schedule (full, incremental)
- SQL AlwaysOn replica information, usage, and health status
- SQL change tracking performance issues, retention period, and autocleanup state

- SQL change tracking retention period
- State and status message performance statistics including most common and most expensive message types
- ***[New]*** Management point traffic statistics (total bytes sent and received by endpoint)
- ***[New]*** Management point performance counter measurements

Miscellaneous

- Configuration of data warehouse service point including synchronization schedule and average time
- Count of scripts and run statistics
- Count of sites with Wake On LAN (WOL)
- Reporting usage and performance statistics
- Phased deployment usage statistics
- Management insights item counts and progress
- Count of crashes for unique non-Configuration Manager processes on the site server, and Watson signature ID, if available

Level 3 - Full

The Full level includes all data in the Basic and Enhanced levels. It also includes additional information about Endpoint Protection, update compliance percentages, and software update information. This level can also include advanced diagnostic information like system files and memory snapshots. This advanced data might include personal information exists in memory or log files at the time of capture.

For Configuration Manager version 1810, this level includes the following data:

- Automatic deployment rule evaluation schedule information
- ATP health summary
- Collection evaluation and refresh statistics
- Compliance policy statistics on compliance and errors
- Compliance settings: SCEP, VPN, Wi-Fi, and compliance policy template configuration details
- DCM config pack for Configuration Manager usage
- Detailed client deployment installation errors
- Endpoint Protection health summary: including count of protected, at risk, unknown, and unsupported clients
- Endpoint Protection policy configuration
- List of processes configured with installation behavior for applications
- Minimum/maximum/average number of hours since last software update scan
- Minimum/maximum/average number of inactive clients in software update deployment collections
- Minimum/maximum/average number of software updates per package
- MSI product code deployment statistics

- Overall compliance of software update deployments
- Count of groups that have expired software updates
- Software update deployment error codes and counts
- Software update deployment information: percentage of deployments that are targeted with client versus UTC time, required versus optional versus silent, and reboot suppression
- Software update products synced by software update point
- Software update scan success percentages
- Top 50 CPUs in the environment
- Type of Exchange Active Sync (EAS) conditional access policies (block or quarantine) for devices that Microsoft Intune manages
- Microsoft Store for Business application details: non-aggregate list of synced applications including AppID, online state or offline state, and total purchased license counts
- ***[New]*** Count of clients pushed with option to not allow fallback to NTLM

Levels of diagnostic usage data collection for version 1806

7/19/2019 • 13 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager version 1806 collects three levels of diagnostics and usage data: **Basic**, **Enhanced**, and **Full**. By default, this feature is set at the Enhanced level. The following sections provide additional detail about data collected at each level.

Changes from previous versions are noted with ***[New]***, ***[Updated]***, ***[Removed]***, or ***[Moved]***.

> **IMPORTANT**
> Configuration Manager doesn't collect site codes, sites names, IP addresses, user names, computer names, physical addresses, or email addresses on the Basic or Enhanced levels. Any collection of this information on the Full level is not purposeful. It is potentially included in advanced diagnostic information like log files or memory snapshots. Microsoft doesn't use this information to identify you, contact you, or develop advertising.

How to change the level

Administrators who have a role-based administrative scope that includes **Modify** permissions on the **Site** object class can change the level of data collected in the Diagnostics and Usage Data settings in the Configuration Manager console.

You change the data collection level from within the console by navigating to **Administration** > **Overview** > **Site Configuration** > **Sites**. Open **Hierarchy Settings**, and then select the data level you want to use.

Level 1 - Basic

The Basic level includes data about your hierarchy, data that's required to help improve your installation or upgrade experience, and data that helps determine the Configuration Manager updates that are applicable for your hierarchy.

For Configuration Manager version 1806, this level includes the following data:

- Statistics about Configuration Manager console connections: OS version, language, SKU and architecture, system memory, logical processor count, connect site ID, installed .NET versions, and console language packs
- Basic application and deployment type counts: total apps, total apps with multiple deployment types, total apps with dependencies, total superseded apps, and count of deployment technologies in use
- Basic Configuration Manager site hierarchy data: site list, type, version, status, client count, and time zone
- ***[Updated]*** Basic database configuration: processors, memory size, memory settings, Configuration Manager database configuration, Configuration Manager database size, cluster configuration, and configuration of distributed views
- Basic discovery statistics: discovery count, minimum/maximum/average group sizes, and when the site is running entirely with Azure Active Directory Services

- Basic Endpoint Protection information about antimalware client versions
- Basic OS deployment counts of images
- Basic site system server information: site system roles used, internet and SSL status, OS, processors, physical or virtual machine, and usage of site server high availability
- Configuration Manager database schema (hash of all object definitions)
- Configured level for diagnostics and usage data, online or offline mode, and fast update configuration
- Count of client languages and locales
- Count of Configuration Manager client versions, OS versions, and Office versions
- Count of operating systems for managed devices and policies set by the Exchange Connector
- Count of Windows 10 devices by branch and build
- Count of Windows 10 clients that use Windows Update for Business
- Database performance metrics: replication processing information, top SQL Server stored procedures by processor, and disk usage
- Distribution point and management point types and basic configuration information: protected, prestaged, PXE, multicast, SSL state, pull/peer distribution points, MDM-enabled, and SSL-enabled
- Hashed list of extensions to admin console property pages and wizards
- Setup Information:
  - Build, install type, language packs, features that you enabled
  - Pre-release use, setup media type, branch type
  - Software Assurance expiration date
  - Update pack deployment status and errors, download progress, and prerequisite errors
  - Use of update fast ring
  - Version of post-upgrade script
- SQL version, service pack level, edition, collation ID, and character set
- Diagnostics and usage data statistics: when run, runtime, errors
- Whether network discovery is enabled or disabled
- Count of clients joined to Azure Active Directory
- Count of phased deployments created by type
- Count of extended interoperability clients
- Hashed list of hardware inventory properties longer than 255 characters
- ***[Moved]*** Count of clients by co-management enrollment method
- ***[Moved]*** Error statistics for co-management enrollment
- ***[New]*** Count of clients by Windows OS age, to the nearest three-month interval
- ***[New]*** Top 10 processor names used on clients
- ***[New]*** Count and processing rates of key Configuration Manager objects: data discovery records (DDR),

state messages, status messages, hardware inventory, software inventory, and overall count of files in inboxes

- ***[New]*** Site server disk and processor performance information
- ***[New]*** Uptime and memory usage information for Configuration Manager site server processes
- ***[New]*** Count of crashes for Configuration Manager site server processes, and Watson signature ID, if available

Level 2 - Enhanced

The Enhanced level is the default after setup finishes. This level includes data that's collected in the Basic level and feature-specific data (frequency and duration of use), Configuration Manager client settings (component name, state, and certain settings like polling intervals), and basic information about software updates.

This level is recommended because it provides Microsoft with the minimum data that's required to make useful improvements in future versions of products and services. This level doesn't collect object names (sites, users, computer, or objects), details of security-related objects, or vulnerabilities like counts of systems that require software updates.

For Configuration Manager version 1806, this level includes the following data:

Application management

- App requirements: count of built-in conditions referenced by deployment technology
- App supersedence, maximum depth of chain
- Application approval statistics and usage frequency
- Application content size statistics
- Application deployment information: use of install versus uninstall, requires approval, user interaction enabled/disabled, dependency, supersedence, and usage count of install behavior feature
- Application policy size and complexity statistics
- Available application request statistics
- Basic configuration information for packages and programs: deployment options and program flags
- Basic usage/targeting information for deployment types: user versus device targeted, required versus available, and universal apps
- Count of App-V environments and deployment properties
- Count of application applicability by OS
- Count of applications that are referenced by a task sequence
- Count of distinct branding for application catalog
- Count of Office 365 applications created using dashboard
- Count of packages by type
- Count of package/program deployments
- Count of Windows 10 licensed application licenses
- Count of Windows Installer deployment types by uninstall content settings

- Count of Microsoft Store for Business apps and sync statistics: summarized types of apps, licensed app status, and number of online and offline licensed apps
- Maintenance window type and duration
- Minimum/maximum/average number of application deployments per user/device per time period
- Most common application installation error codes by deployment technology
- MSI configuration options and counts
- Statistics on end-user interaction with notification for required software deployments
- Universal Data Access usage, how created
- Aggregated User Device Affinity statistics
- Max and average primary users per device
- ***[New]*** Application global condition usage by type
- ***[New]*** Software Center customization configuration
- ***[New]*** Package Conversion Manager readiness and counts
- ***[New]*** Count of application detection methods by type
- ***[New]*** Count of application enforcement errors
- ***[New]*** MSI installer properties
- ***[New]*** Statistics of user install requests

Client

- Active Management Technology (AMT) client version
- BIOS age in years
- Count of devices with Secure Boot enabled
- Count of devices by TPM state
- Client auto-upgrade: deployment configuration including client piloting and exclusion usage (extended interoperability client)
- Client cache size configuration
- Client deployment download errors
- ***[Updated]*** Client health statistics and top issue summary by client version
- Client notification operation action status: how many times each is run, max number of targeted clients, and average success rate
- Count of client installations from each source location type
- Count of client installation failures
- Count of devices virtualized by Hyper-V or Azure
- Count of Software Center actions
- Count of UEFI-enabled devices
- Deployment methods used for client and count of clients per deployment method

- List/count of enabled client agents
- OS age in months
- Number of hardware inventory classes, software inventory rules, and file collection rules
- Statistics for device health attestation: most common error codes, number of on-premises servers, and counts of devices in various states
- Count of devices by default browser
- ***[New]*** Count of Configuration Manager-generated server authentication certificates
- ***[New]*** Count of Microsoft Surface devices by model

Cloud Services

- Azure Active Directory discovery statistics
- Configuration and usage statistics of Cloud Management Gateway: counts of regions and environments, and authentication/authorization statistics
- Count of Azure Active Directory applications and services connected to Configuration Manager
- Count of collections synced to Azure Log Analytics
- Count of Upgrade Analytics Connectors
- Whether the Azure Log Analytics cloud connector is enabled
- ***[New]*** Count of pull-distribution points with a cloud distribution point as a source location

Co-management

- Aggregated usage statistics of co-management: number of enrolled clients, clients receiving policy, workload states, pilot/exclusion collection sizes, and enrollment errors
- Enrollment schedule and historical statistics
- Count of clients eligible for co-management
- Associated Microsoft Intune tenant

Collections

- Collection ID usage (not running out of IDs)
- Collection evaluation statistics: query time, assigned versus unassigned counts, counts by type, ID rollover, and rule usage
- Collections without a deployment

Compliance settings

- Basic configuration baseline information: count, number of deployments, and number of references
- Compliance policy error statistics
- Count of configuration items by type
- Count of deployments that reference built-in settings, including remediate setting
- Count of rules and deployments created for custom settings, including remediate setting
- Count of deployed Simple Certificate Enrollment Protocol (SCEP), VPN, Wi-Fi, certificate (.pfx), and compliance policy templates

- Count of SCEP certificate, VPN, Wi-Fi, certificate (.pfx), and compliance policy deployments by platform
- Windows Hello for Business policy (created, deployed)
- ***[New]*** Count of deployed Microsoft Edge browser policies

Content

- Boundary group statistics: how many fast, how many slow, count per group, and fallback relationships
- Boundary group information: count of boundaries and site systems that are assigned to each boundary group
- Boundary group relationships and fallback configuration
- Client content download statistics
- Count of boundaries by type
- Count of peer cache clients, usage statistic, and partial download statistics
- Distribution Manager configuration information: threads, retry delay, number of retries, and pull distribution point settings
- Distribution point configuration information: use of branch cache and distribution point monitoring
- Distribution point group information: count of packages and distribution points that are assigned to each distribution point group
- ***[New]*** Content library type, whether local or remote

Endpoint Protection

- Microsoft Defender Advanced Threat Protection (ATP) policies (formerly known as Windows Defender ATP): count of policies, and whether policies are deployed.
- Count of alerts that are configured for Endpoint Protection feature
- Count of collections that are selected to appear in Endpoint Protection dashboard
- Count of Windows Defender Exploit Guard policies, deployments, and targeted clients
- Endpoint Protection deployment errors, count of Endpoint Protection policy deployment error codes
- Endpoint Protection antimalware and Windows Firewall policy usage (number of unique policies assigned to group)

  This data doesn't include any information about the settings included in the policy.

Migration

- Count of migrated objects (use of migration wizard)

Mobile device management (MDM)

- Count of issued mobile device actions: lock, pin rest, wipe, retire, and sync now commands
- Count of mobile device policies
- Count of mobile devices that are managed by Configuration Manager and Microsoft Intune and how they were enrolled (bulk, user-based)
- Count of users who have multiple enrolled mobile devices
- Mobile device polling schedule and statistics for mobile device check-in duration

Microsoft Intune troubleshooting

- Count and size of device actions (wipe, retire, lock), usage data, and data messages that are replicated to Microsoft Intune
- Count and size of state, status, inventory, RDR, DDR, UDX, Tenant state, POL, LOG, Cert, CRP, Resync, CFD, RDO, BEX, ISM, and compliance messages that are downloaded from Microsoft Intune
- Full and delta user synchronization statistics for Microsoft Intune

On-premises mobile device management (MDM)

- Count of Windows 10 bulk enrollment packages and profiles
- Deployment success/failure statistics for on-premises MDM application deployments

OS deployment

- Count of boot images, drivers, driver packages, multicast-enabled distribution points, PXE-enabled distribution points, and task sequences
- Count of boot images by Configuration Manager client version
- Count of boot images by Windows PE version
- Count of edition upgrade policies
- Count of hardware identifiers excluded from PXE
- Count of OS deployment by OS version
- Count of OS upgrades over time
- Count of task sequence deployments using option to pre-download content
- Counts of task sequence step usage
- Version of Windows ADK installed
- ***[New]*** Count of image servicing tasks

Site updates

- Versions of installed Configuration Manager hotfixes

Software Updates

- Available and deadline deltas that are used in automatic deployment rules
- Average and maximum number of assignments per update
- Client update evaluation and scan schedules
- Classifications that are synced by software update point
- Cluster patching statistics
- Configuration of Windows 10 express updates
- Configurations that are used for active Windows 10 servicing plans
- Count of deployed Office 365 updates
- Count of Microsoft Surface drivers synced
- Count of update groups and assignments
- Count of update packages and the maximum/minimum/average number of distribution points that are

targeted with packages

- Count of updates that are created and deployed with System Center Update Publisher
- Count of Windows Update for Business policies created and deployed
- Aggregated statistics of Windows Update for Business configurations
- Number of automatic deployment rules that are tied to synchronization
- Number of automatic deployment rules that create new or add updates to an existing group
- Number of automatic deployment rules that have multiple deployments
- Number of update groups and minimum/maximum/average number of updates per group
- Number of updates and percentage of updates that are deployed, expired, superseded, downloaded, and contain EULAs
- Software update point load balancing statistics
- Software update point synchronization schedule
- Total/average number of collections that have software update deployments and the maximum/average number of deployed updates
- Update scan error codes and machine count
- Windows 10 dashboard content versions
- ***[New]*** Count of third-party software update catalog subscriptions and usage
- ***[New]*** Count of software updates deployed with and without content

SQL/performance data

- Configuration and duration of site summarization
- Count of largest database tables
- Discovery operational statistics (count of objects found)
- Discovery types, enabled, and schedule (full, incremental)
- SQL AlwaysOn replica information, usage, and health status
- SQL change tracking performance issues, retention period, and auto-cleanup state
- SQL change tracking retention period
- State and status message performance statistics including most common and most expensive message types

Miscellaneous

- Configuration of data warehouse service point including synchronization schedule and average time
- Count of scripts and run statistics
- Count of sites with Wake On LAN (WOL)
- Reporting usage and performance statistics
- Phased deployment usage statistics
- ***[New]*** CMPivot usage statistics

- ***[New]*** Management insights item counts and progress
- ***[New]*** Count of crashes for unique non-Configuration Manager processes on the site server, and Watson signature ID, if available

Level 3 - Full

The Full level includes all data in the Basic and Enhanced levels. It also includes additional information about Endpoint Protection, update compliance percentages, and software update information. This level can also include advanced diagnostic information like system files and memory snapshots, which might include personal information that existed in memory or log files at the time of capture.

For Configuration Manager version 1806, this level includes the following data:

- Automatic deployment rule evaluation schedule information
- ATP Health Summary
- Collection evaluation and refresh statistics
- Compliance policy statistics on compliance and errors
- Compliance Settings: SCEP, VPN, Wi-Fi, and compliance policy template configuration details
- DCM config pack for System Center Configuration Manager usage
- Detailed client deployment installation errors
- Endpoint Protection health summary: including count of protected, at risk, unknown, and unsupported clients
- Endpoint Protection policy configuration
- List of processes configured with installation behavior for applications
- Minimum/maximum/average number of hours since last software update scan
- Minimum/maximum/average number of inactive clients in software update deployment collections
- Minimum/maximum/average number of software updates per package
- MSI product code deployment statistics
- Overall compliance of software update deployments
- Count of groups that have expired software updates
- Software update deployment error codes and counts
- Software update deployment information: percentage of deployments that are targeted with client versus UTC time, required versus optional versus silent, and reboot suppression
- Software update products synced by software update point
- Software update scan success percentages
- Top 50 CPUs in the environment
- Type of Exchange Active Sync (EAS) conditional access policies (block or quarantine) for devices that Microsoft Intune manages
- Microsoft Store for Business application details: non-aggregate list of synced applications including AppID, online state or offline state, and total purchased license counts

Levels of diagnostic usage data collection for version 1802 of System Center Configuration Manager

7/19/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager version 1802 collects three levels of diagnostics and usage data: **Basic**, **Enhanced**, and **Full**. By default, this feature is set at the Enhanced level. The following sections provide additional detail about data collected at each level.

Changes from previous versions are noted with ***[New]***, ***[Updated]***, ***[Removed]***, or ***[Moved]***.

> **IMPORTANT**
> Configuration Manager doesn't collect site codes, sites names, IP addresses, user names, computer names, physical addresses, or email addresses on the Basic or Enhanced levels. Any collection of this information on the Full level is not purposeful. It is potentially included in advanced diagnostic information like log files or memory snapshots. Microsoft doesn't use this information to identify you, contact you, or develop advertising.

How to change the level

Administrators who have a role-based administrative scope that includes **Modify** permissions on the **Site** object class can change the level of data collected in the Diagnostics and Usage Data settings in the Configuration Manager console.

You change the data collection level from within the console by navigating to **Administration** > **Overview** > **Site Configuration** > **Sites**. Open **Hierarchy Settings**, and then select the data level you want to use.

Level 1 - Basic

The Basic level includes data about your hierarchy, data that's required to help improve your installation or upgrade experience, and data that helps determine the Configuration Manager updates that are applicable for your hierarchy.

For Configuration Manager version 1802, this level includes the following data:

- Statistics about Configuration Manager console connections: OS version, language, SKU and architecture, system memory, logical processor count, connect site ID, installed .NET versions, and console language packs
- Basic application and deployment type counts: total apps, total apps with multiple deployment types, total apps with dependencies, total superseded apps, and count of deployment technologies in use
- Basic Configuration Manager site hierarchy data: site list, type, version, status, client count, and time zone
- Basic database configuration: processors, cluster configuration, and configuration of distributed views
- Basic discovery statistics: discovery count, minimum/maximum/average group sizes, and when the site is running entirely with Azure Active Directory Services
- Basic Endpoint Protection information about antimalware client versions
- Basic OS deployment counts of images

- Basic site system server information: site system roles used, internet and SSL status, OS, processors, physical or virtual machine, and usage of site server high availability
- Configuration Manager database schema (hash of all object definitions)
- Configured telemetry level, online or offline mode, and fast update configuration
- Count of client languages and locales
- Count of Configuration Manager client versions, OS versions, and Office versions
- Count of operating systems for managed devices and policies set by the Exchange Connector
- Count of Windows 10 devices by branch and build
- ***[Moved]*** Count of Windows 10 clients that use Windows Update for Business
- Database performance metrics: replication processing information, top SQL Server stored procedures by processor, and disk usage
- Distribution point and management point types and basic configuration information: protected, prestaged, PXE, multicast, SSL state, pull/peer distribution points, MDM-enabled, and SSL-enabled
- Hashed list of extensions to admin console property pages and wizards
- Setup Information:
  - Build, install type, language packs, features that you enabled
  - Pre-release use, setup media type, branch type
  - Software Assurance expiration date
  - Update pack deployment status and errors, download progress, and prerequisite errors
  - Use of update fast ring
  - Version of post-upgrade script
- SQL version, service pack level, edition, collation ID, and character set
- Telemetry statistics: when run, runtime, errors
- Whether network discovery is enabled or disabled
- ***[Moved]*** Count of clients joined to Azure Active Directory
- ***[New]*** Count of phased deployments created by type
- ***[New]*** Count of extended interoperability clients
- ***[New]*** Hashed list of hardware inventory properties longer than 255 characters

Level 2 - Enhanced

The Enhanced level is the default after setup finishes. This level includes data that's collected in the Basic level and feature-specific data (frequency and duration of use), Configuration Manager client settings (component name, state, and certain settings like polling intervals), and basic information about software updates.

This level is recommended because it provides Microsoft with the minimum data that's required to make useful improvements in future versions of products and services. This level does not collect object names (sites, users, computer, or objects), details of security-related objects, or vulnerabilities like counts of systems that require software updates.

For Configuration Manager version 1802, this level includes the following data:

Application management

- App requirements: count of built-in conditions referenced by deployment technology
- App supersedence, maximum depth of chain
- Application approval statistics and usage frequency
- Application content size statistics
- Application deployment information: use of install versus uninstall, requires approval, user interaction enabled/disabled, dependency, supersedence, and usage count of install behavior feature
- Application policy size and complexity statistics
- Available application request statistics
- Basic configuration information for packages and programs: deployment options and program flags
- Basic usage/targeting information for deployment types: user versus device targeted, required versus available, and universal apps
- Count of App-V environments and deployment properties
- Count of application applicability by OS
- Count of applications that are referenced by a task sequence
- Count of distinct branding for application catalog
- Count of Office 365 applications created using dashboard
- Count of packages by type
- Count of package/program deployments
- Count of Windows 10 licensed application licenses
- Count of Windows Installer deployment types by uninstall content settings
- Count of Microsoft Store for Business apps and sync statistics: summarized types of apps, licensed app status, and number of online and offline licensed apps
- Maintenance window type and duration
- Minimum/maximum/average number of application deployments per user/device per time period
- Most common application installation error codes by deployment technology
- MSI configuration options and counts
- Statistics on end-user interaction with notification for required software deployments
- Universal Data Access usage, how created
- ***[New]*** Aggregated User Device Affinity statistics
- ***[New]*** Max and average primary users per device

Client

- Active Management Technology (AMT) client version
- BIOS age in years

- Count of devices with Secure Boot enabled
- Count of devices by TPM state
- Client auto-upgrade: deployment configuration including client piloting and exclusion usage (extended interoperability client)
- Client cache size configuration
- Client deployment download errors
- Client health statistics and top issue summary
- Client notification operation action status: how many times each is run, max number of targeted clients, and average success rate
- Count of client installations from each source location type
- Count of client installation failures
- Count of devices virtualized by Hyper-V or Azure
- Count of Software Center actions
- Count of UEFI-enabled devices
- Deployment methods used for client and count of clients per deployment method
- List/count of enabled client agents
- OS age in months
- Number of hardware inventory classes, software inventory rules, and file collection rules
- Statistics for device health attestation: most common error codes, number of on-premises servers, and counts of devices in various states
- ***[New]*** Count of devices by default browser

Cloud Services

- Azure Active Directory discovery statistics
- Configuration and usage statistics of Cloud Management Gateway: counts of regions and environments, and authentication/authorization statistics
- Count of Azure Active Directory applications and services connected to Configuration Manager
- Count of collections synced to Azure Log Analytics
- Count of Upgrade Analytics Connectors
- Whether the Azure Log Analytics cloud connector is enabled

Co-management

- Aggregated usage statistics of co-management: number of enrolled clients, clients receiving policy, workload states, pilot/exclusion collection sizes, and enrollment errors
- Count of clients by co-management enrollment method
- Error statistics for co-management enrollment
- Enrollment schedule and historical statistics
- Count of clients eligible for co-management

- Associated Microsoft Intune tenant

Collections

- Collection ID usage (not running out of IDs)
- Collection evaluation statistics: query time, assigned versus unassigned counts, counts by type, ID rollover, and rule usage
- Collections without a deployment

Compliance settings

- Basic configuration baseline information: count, number of deployments, and number of references
- Compliance policy error statistics
- Count of configuration items by type
- Count of deployments that reference built-in settings, including remediate setting
- Count of rules and deployments created for custom settings, including remediate setting
- Count of deployed Simple Certificate Enrollment Protocol (SCEP), VPN, Wi-Fi, certificate (.pfx), and compliance policy templates
- Count of SCEP certificate, VPN, Wi-Fi, certificate (.pfx) and compliance policy deployments by platform
- Windows Hello for Business policy (created, deployed)

Content

- ***[Updated]*** Boundary group statistics: how many fast, how many slow, count per group, and fallback relationships
- Boundary group information: count of boundaries and site systems that are assigned to each boundary group
- Boundary group relationships and fallback configuration
- Client content download statistics
- Count of boundaries by type
- Count of peer cache clients, usage statistic, and partial download statistics
- Distribution Manager configuration information: threads, retry delay, number of retries, and pull distribution point settings
- Distribution point configuration information: use of branch cache and distribution point monitoring
- Distribution point group information: count of packages and distribution points that are assigned to each distribution point group

Endpoint Protection

- Microsoft Defender Advanced Threat Protection (ATP) policies (formerly known as Windows Defender ATP): count of policies, and whether policies are deployed.
- Count of alerts that are configured for Endpoint Protection feature
- Count of collections that are selected to appear in Endpoint Protection dashboard
- Count of Windows Defender Exploit Guard policies, deployments, and targeted clients
- Endpoint Protection deployment errors, count of Endpoint Protection policy deployment error codes

- Endpoint Protection antimalware and Windows Firewall policy usage (number of unique policies assigned to group)

  This data doesn't include any information about the settings included in the policy.

Migration

- Count of migrated objects (use of migration wizard)

Mobile device management (MDM)

- Count of issued mobile device actions: lock, pin rest, wipe, retire, and sync now commands
- Count of mobile device policies
- Count of mobile devices that are managed by Configuration Manager and Microsoft Intune and how they were enrolled (bulk, user-based)
- Count of users who have multiple enrolled mobile devices
- Mobile device polling schedule and statistics for mobile device check-in duration

Microsoft Intune troubleshooting

- Count and size of device actions (wipe, retire, lock), telemetry, and data messages that are replicated to Microsoft Intune
- Count and size of state, status, inventory, RDR, DDR, UDX, Tenant state, POL, LOG, Cert, CRP, Resync, CFD, RDO, BEX, ISM, and compliance messages that are downloaded from Microsoft Intune
- Full and delta user synchronization statistics for Microsoft Intune

On-premises mobile device management (MDM)

- Count of Windows 10 bulk enrollment packages and profiles
- Deployment success/failure statistics for on-premises MDM application deployments

OS deployment

- Count of boot images, drivers, driver packages, multicast-enabled distribution points, PXE-enabled distribution points, and task sequences
- Count of boot images by Configuration Manager client version
- Count of boot images by Windows PE version
- Count of edition upgrade policies
- Count of hardware identifiers excluded from PXE
- Count of OS deployment by OS version
- Count of OS upgrades over time
- Count of task sequence deployments using option to pre-download content
- Counts of task sequence step usage
- Version of Windows ADK installed

Site updates

- Versions of installed Configuration Manager hotfixes

Software Updates

- Available and deadline deltas that are used in automatic deployment rules

- Average and maximum number of assignments per update
- Client update evaluation and scan schedules
- Classifications that are synced by software update point
- Cluster patching statistics
- Configuration of Windows 10 express updates
- Configurations that are used for active Windows 10 servicing plans
- Count of deployed Office 365 updates
- Count of Microsoft Surface drivers synced
- Count of update groups and assignments
- Count of update packages and the maximum/minimum/average number of distribution points that are targeted with packages
- Count of updates that are created and deployed with System Center Update Publisher
- Count of Windows Update for Business policies created and deployed
- ***[New]*** Aggregated statistics of Windows Update for Business configurations
- Number of automatic deployment rules that are tied to synchronization
- Number of automatic deployment rules that create new or add updates to an existing group
- Number of automatic deployment rules that have multiple deployments
- Number of update groups and minimum/maximum/average number of updates per group
- Number of updates and percentage of updates that are deployed, expired, superseded, downloaded, and contain EULAs
- Software update point load balancing statistics
- Software update point synchronization schedule
- Total/average number of collections that have software update deployments and the maximum/average number of deployed updates
- Update scan error codes and machine count
- Windows 10 dashboard content versions

SQL/performance data

- Configuration and duration of site summarization
- Count of largest database tables
- Discovery operational statistics (count of objects found)
- Discovery types, enabled, and schedule (full, incremental)
- SQL AlwaysOn replica information, usage, and health status
- SQL change tracking performance issues, retention period, and auto-cleanup state
- SQL change tracking retention period
- State and status message performance statistics including most common and most expensive message

types

Miscellaneous

- Configuration of data warehouse service point including synchronization schedule and average time
- Count of scripts and run statistics
- Count of sites with Wake On LAN (WOL)
- Reporting usage and performance statistics
- ***[New]*** Phased deployment usage statistics

Level 3 - Full

The Full level includes all data in the Basic and Enhanced levels. It also includes additional information about Endpoint Protection, update compliance percentages, and software update information. This level can also include advanced diagnostic information like system files and memory snapshots, which might include personal information that existed in memory or log files at the time of capture.

For Configuration Manager version 1802, this level includes the following data:

- Automatic deployment rule evaluation schedule information
- ATP Health Summary
- Collection evaluation and refresh statistics
- Compliance policy statistics on compliance and errors
- Compliance Settings: SCEP, VPN, Wi-Fi, and compliance policy template configuration details
- DCM config pack for System Center Configuration Manager usage
- Detailed client deployment installation errors
- Endpoint Protection health summary: including count of protected, at risk, unknown, and unsupported clients
- Endpoint Protection policy configuration
- List of processes configured with installation behavior for applications
- Minimum/maximum/average number of hours since last software update scan
- Minimum/maximum/average number of inactive clients in software update deployment collections
- Minimum/maximum/average number of software updates per package
- ***[Updated]*** MSI product code deployment statistics
- Overall compliance of software update deployments
- Count of groups that have expired software updates
- Software update deployment error codes and counts
- Software update deployment information: percentage of deployments that are targeted with client versus UTC time, required versus optional versus silent, and reboot suppression
- Software update products synced by software update point
- Software update scan success percentages

- Top 50 CPUs in the environment
- Type of Exchange Active Sync (EAS) conditional access policies (block or quarantine) for devices that Microsoft Intune manages
- Microsoft Store for Business application details: non-aggregate list of synced applications including AppID, online state or offline state, and total purchased license counts

How diagnostics and usage data is collected by System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To collect diagnostics and usage data for System Center Configuration Manager, each primary site runs SQL Server queries on a weekly basis. In a multi-site hierarchy, the data is replicated to the central administration site.

At the top-level site of a hierarchy, the service connection point site system role submits this information when it checks for updates. The mode of the service connection point detemines how the data is transferred:

- **In online mode:** Diagnostics and usage data is automatically sent once a week from the service connection point to the cloud service.
- **In offline mode:** Diagnostics and usage data is transferred manually by using the service connection tool. For more information, see Use the Service Connection Tool for System Center Configuration Manager.

For more information, see About the service connection point in System Center Configuration Manager.

How to view diagnostics and usage data for Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can view diagnostic and usage data from your Configuration Manager hierarchy to confirm that it includes no sensitive or identifiable information. The site summarizes and stores its diagnostic data in the **TEL_TelemetryResults** table of the site database. It formats the data to be programmatically usable and efficient.

The information in this article gives you a view of the exact data sent to Microsoft. It's not intended to be used for other purposes, like data analysis.

View data in database

Use the following SQL command to view the contents of this table and show the exact data that's sent:

```
SELECT * FROM TEL_TelemetryResults
```

Export the data

When the service connection point is in offline mode, use the service connection tool to export the current data to a comma-separated values (CSV) file. Run the service connection tool on the service connection point with the **-Export** parameter.

For more information, see Use the service connection tool.

One-way hashes

Some data consists of strings of random alphanumeric characters. Configuration Manager uses the SHA-256 algorithm to create one-way hashes. This process makes sure that Microsoft doesn't collect potentially sensitive data. The hashed data can still be used for correlation and comparison purposes.

For example, instead of collecting the names of tables in the site database, it captures the one-way hash for each table name. This behavior makes sure that any custom table names aren't visible. Microsoft then does the same one-way hash process of the default SQL table names. Comparing the results of the two queries determines the deviation of your database schema from the product default. This information is then used to improve updates that require changes to the SQL schema.

When you view the raw data, a common hashed value appears in each row of data. This hash is the hierarchy ID. It's used to correlate data with the same hierarchy without identifying the customer or source.

How the one-way hash works

1. Get your hierarchy ID by running the following SQL query in SQL Management Studio against the Configuration Manager database:

   ```
   select [dbo].[fnGetHierarchyID]()
   ```

2. Use the following Windows PowerShell script to do the one-way hash of your hierarchy ID.

```
Param( [Parameter(Mandatory=$True)] [string]$value )
  $guid = [System.Guid]::NewGuid()
  if( [System.Guid]::TryParse($value,[ref] $guid) -eq $true ) {
  #many of the values we hash are Guids
  $bytesToHash = $guid.ToByteArray()
} else {
  #otherwise hash as string (unicode)
  $ue = New-Object System.Text.UnicodeEncoding
  $bytesToHash = $ue.GetBytes($value)
}
  # Load Hash Provider (https://en.wikipedia.org/wiki/SHA-2)
$hashAlgorithm = [System.Security.Cryptography.SHA256Cng]::Create()
# Hash the input
$hashedBytes = $hashAlgorithm.ComputeHash($bytesToHash)
# Base64 encode the result for transport
$result = [Convert]::ToBase64String($hashedBytes)
return $result
```

3. Compare the script output against the GUID in the raw data. This process shows how the data is obscured.

Customer Experience Improvement Program (CEIP) for System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

> **NOTE**
> Starting in Configuration Manager version 1802 the CEIP feature is removed from the product.

During installation of the Configuration Manager console, you can choose to participate in the **Customer Experience Improvement Program** (CEIP). CEIP is turned off by default. If it was previously enabled, it remains enabled.

- CEIP is separate from Diagnostics and usage data for System Center Configuration Manager.
- CEIP is per console. It collects data such as the number of times that each element is selected in the user interface.
- Read the privacy statement.

Change the CEIP settings per console installation. To change the settings, go to the console's backstage tab (the upper left tab with the drop-down arrow), and select **Customer Experience Improvement Program**.

Security and privacy for System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article includes resources for Security and Privacy for System Center Configuration Manager.

Before proceeding, ensure that you learn the Fundamentals of System Center Configuration Manager. If you already installed System Center Configuration Manager, identify the design decisions for your implementation. You might find the Configuration Manager planning and deployment content helpful.

See the following articles for security-related features in the product:

- Security and privacy for operating system deployment in System Center Configuration Manager
- Security and privacy for application management in System Center Configuration Manager
- Security and privacy for software updates in System Center Configuration Manager
- Security and privacy for compliance settings in System Center Configuration Manager
- Endpoint Protection in System Center Configuration Manager
- Security and privacy for collections in System Center Configuration Manager
- Security and privacy for queries in System Center Configuration Manager
- Security and privacy for power management in System Center Configuration Manager
- Security and privacy for remote control in System Center Configuration Manager
- Security and privacy for hardware inventory in System Center Configuration Manager
- Security and privacy for software inventory in System Center Configuration Manager
- Security and privacy for Asset Intelligence in System Center Configuration Manager
- Security and privacy for reporting in System Center Configuration Manager

Security and privacy articles:

- Plan for security in System Center Configuration Manager
- Configure security in System Center Configuration Manager
- Security best practices and privacy information for System Center Configuration Manager
- Cryptographic controls technical reference for System Center Configuration Manager
- Ports used in System Center Configuration Manager
- Accounts used in System Center Configuration Manager

Plan for security in Configuration Manager

7/26/2019 • 21 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article describes the concepts for you to consider when planning for security with your Configuration Manager implementation. It includes the following sections:

Plan for certificates (self-signed and PKI)

Configuration Manager uses a combination of self-signed certificates and public key infrastructure (PKI) certificates.

Use PKI certificates whenever possible. For more information, see PKI certificate requirements. When Configuration Manager requests PKI certificates during enrollment for mobile devices, you must use Active Directory Domain Services and an enterprise certification authority. For all other PKI certificates, deploy and manage them independently from Configuration Manager.

PKI certificates are required when client computers connect to internet-based site systems. Some scenarios with the cloud management gateway and cloud distribution point also require PKI certificates. For more information, see Manage clients on the internet.

When you use a PKI, you can also use IPsec to help secure the server-to-server communication between site systems in a site, between sites, and for other data transfer between computers. Implementation of IPsec is independent from Configuration Manager.

When PKI certificates aren't available, Configuration Manager automatically generates self-signed certificates. Some certificates in Configuration Manager are always self-signed. In most cases, Configuration Manager automatically manages the self-signed certificates, and you don't have to take additional action. One example is the site server signing certificate. This certificate is always self-signed. It makes sure that the policies that clients download from the management point were sent from the site server and weren't tampered with.

Cryptography: Next Generation (CNG) certificates

Configuration Manager supports Cryptography: Next Generation (CNG) certificates. Configuration Manager clients can use PKI client authentication certificate with private key in CNG Key Storage Provider (KSP). With KSP support, Configuration Manager clients support hardware-based private key, such as TPM KSP for PKI client authentication certificates. For more information, see CNG certificates overview.

Enhanced HTTP

Using HTTPS communication is recommended for all Configuration Manager communication paths, but is challenging for some customers due to the overhead of managing PKI certificates. The introduction of Azure Active Directory (Azure AD) integration reduces some but not all of the certificate requirements. Starting in version 1806, you can enable the site to use **Enhanced HTTP**. This configuration supports HTTPS on site systems by using a combination of self-signed certificates and Azure AD. It doesn't require PKI. For more information, see Enhanced HTTP.

Certificates for CMG and CDP

Managing clients on the internet via the cloud management gateway (CMG) and cloud distribution point (CDP) requires the use of certificates. The number and type of certificates varies depending upon your specific scenarios. For more information, see the following articles:

- Certificates for the cloud management gateway
- Certificates for the cloud distribution point

Plan for the site server signing certificate (self-signed)

Clients can securely get a copy of the site server signing certificate from Active Directory Domain Services and from client push installation. If clients can't get a copy of this certificate by one of these mechanisms, install it when you install the client. This process is especially important if the client's first communication with the site is with an internet-based management point. Because this server is connected to an untrusted network, it's more vulnerable to attack. If you don't take this additional step, clients automatically download a copy of the site server signing certificate from the management point.

Clients can't securely get a copy of the site server certificate in the following scenarios:

- You don't install the client by using client push, and:
  - You haven't extended the Active Directory schema for Configuration Manager.
  - You haven't published the client's site to Active Directory Domain Services.
  - The client is from an untrusted forest or a workgroup.
- You're using internet-based client management and you install the client when it's on the internet.

To install clients with a copy of the site server signing certificate

1. Locate the site server signing certificate on the primary site server. The certificate is stored in the **SMS** certificate store of Windows. It has the Subject name **Site Server** and the friendly name, **Site Server Signing Certificate**.
2. Export the certificate without the private key, store the file securely, and access it only from a secured channel.
3. Install the client by using the following client.msi property: `SMSSIGNCERT=<full path and file name>`

Plan for PKI certificate revocation

When you use PKI certificates with Configuration Manager, plan for use of a certificate revocation list (CRL). Devices use the CRL to verify the certificate on the connecting computer. The CRL is a file that a certificate authority (CA) creates and signs. It has a list of certificates that the CA has issued but revoked. When a certificate administrator revokes certificates, its thumbprint is added to the CRL. For example, if an issued certificate is known or suspected to be compromised.

> **IMPORTANT**
> Because the location of the CRL is added to a certificate when a CA issues it, ensure that you plan for the CRL before you deploy any PKI certificates that Configuration Manager uses.

IIS always checks the CRL for client certificates, and you can't change this configuration in Configuration Manager. By default, Configuration Manager clients always check the CRL for site systems. Disable this setting by specifying a site property and by specifying a CCMSetup property.

Computers that use certificate revocation checking but can't locate the CRL behave as if all certificates in the certification chain are revoked. This behavior is due to the fact that they can't verify if the certificates are in the certificate revocation list. In this scenario, all connections fail that require certificates and include CRL checking. When validating that your CRL is accessible by browsing to its http location, it is important to note that the Configuration Manager client runs as LOCAL SYSTEM. Therefore, testing CRL accessibility with a web browser running under user context may succeed, however the computer account may be blocked when attempting to make an http connection to the same CRL URL due to the internal web filtering solution. Whitelisting the CRL URL on any web filtering solutions may be necessary in this situation.

Checking the CRL every time that a certificate is used offers more security against using a certificate that's revoked. Although it introduces a connection delay and additional processing on the client. Your organization may require this additional security check for clients on the internet or an untrusted network.

Consult your PKI administrators before you decide whether Configuration Manager clients must check the CRL. Then consider keeping this option enabled in Configuration Manager when both of the following conditions are true:

- Your PKI infrastructure supports a CRL, and it's published where all Configuration Manager clients can locate it. These clients might include devices on the internet, and ones in untrusted forests.
- The requirement to check the CRL for each connection to a site system that's configured to use a PKI certificate is greater than the following requirements:
  - Faster connections
  - Efficient processing on the client
  - The risk of clients failing to connect to servers if the CRL cannot be located

Plan for the PKI trusted root certificates and the certificate issuers list

If your IIS site systems use PKI client certificates for client authentication over HTTP, or for client authentication and encryption over HTTPS, you might have to import root CA certificates as a site property. Here are the two scenarios:

- You deploy operating systems by using Configuration Manager, and the management points only accept HTTPS client connections.
- You use PKI client certificates that don't chain to a root certificate that the management points trust.

> **NOTE**
> When you issue client PKI certificates from the same CA hierarchy that issues the server certificates that you use for management points, you don't have to specify this root CA certificate. However, if you use multiple CA hierarchies and you aren't sure whether they trust each other, import the root CA for the clients' CA hierarchy.

If you must import root CA certificates for Configuration Manager, export them from the issuing CA or from the client computer. If you export the certificate from the issuing CA that's also the root CA, make sure you don't export the private key. Store the exported certificate file in a secure location to prevent tampering. You need access

to the file when you set up the site. If you access the file over the network, make sure the communication is protected from tampering by using IPsec.

If any root CA certificate that you import is renewed, you must import the renewed certificate.

These imported root CA certificates and the root CA certificate of each management point create the certificate issuers list that Configuration Manager computers use in the following ways:

- When clients connect to management points, the management point verifies that the client certificate is chained to a trusted root certificate in the site's certificate issuers list. If it doesn't, the certificate is rejected, and the PKI connection fails.
- When clients select a PKI certificate and have a certificate issuers list, they select a certificate that chains to a trusted root certificate in the certificate issuers list. If there's no match, the client doesn't select a PKI certificate. For more information, see Plan for PKI client certificate selection.

Plan for PKI client certificate selection

If your IIS site systems use PKI client certificates for client authentication over HTTP or for client authentication and encryption over HTTPS, plan for how Windows clients select the certificate to use for Configuration Manager.

> **NOTE**
> Some devices don't support a certificate selection method. Instead, they automatically select the first certificate that fulfills the certificate requirements. For example, clients on Mac computers and mobile devices don't support a certificate selection method.

In many cases, the default configuration and behavior is sufficient. The Configuration Manager client on Windows computers filters multiple certificates by using these criteria in this order:

1. The certificate issuers list: The certificate chains to a root CA that's trusted by the management point.
2. The certificate is in the default certificate store of **Personal**.
3. The certificate is valid, not revoked, and not expired. The validity check also verifies that the private key is accessible.
4. The certificate has client authentication capability, or it's issued to the computer name.
5. The certificate has the longest validity period.

Configure clients to use the certificate issuers list by using the following mechanisms:

- Publish it with Configuration Manager site information to Active Directory Domain Services.
- Install clients by using client push.
- Clients download it from the management point after they're successfully assigned to their site.
- Specify it during client installation as a CCMSetup client.msi property of CCMCERTISSUERS.

Clients that don't have the certificate issuers list when they're first installed and aren't yet assigned to the site skip this check. When clients do have the certificate issuers list and don't have a PKI certificate that chains to a trusted root certificate in the certificate issuers list, certificate selection fails. Clients don't continue with the other certificate selection criteria.

In most cases, the Configuration Manager client correctly identifies a unique and appropriate PKI certificate. However, when this behavior isn't the case, instead of selecting the certificate based on the client authentication capability, you can set up two alternative selection methods:

- A partial string match on the client certificate subject name. This method is a case-insensitive match. It's

appropriate if you're using the fully qualified domain name (FQDN) of a computer in the subject field and want the certificate selection to be based on the domain suffix, for example **contoso.com**. However, you can use this selection method to identify any string of sequential characters in the certificate subject name that differentiates the certificate from others in the client certificate store.

> **NOTE**
>
> You can't use the partial string match with the subject alternative name (SAN) as a site setting. Although you can specify a partial string match for the SAN by using CCMSetup, it'll be overwritten by the site properties in the following scenarios:
>
> - Clients retrieve site information that's published to Active Directory Domain Services.
>   - Clients are installed by using client push installation.
>
>   Use a partial string match in the SAN only when you install clients manually and when they don't retrieve site information from Active Directory Domain Services. For example, these conditions apply to internet-only clients.

- A match on the client certificate subject name attribute values or the subject alternative name (SAN) attribute values. This method is a case-sensitive match. It's appropriate if you're using an X500 distinguished name or equivalent object identifiers (OIDs) in compliance with RFC 3280, and you want the certificate selection to be based on the attribute values. You can specify only the attributes and their values that you require to uniquely identify or validate the certificate and differentiate the certificate from others in the certificate store.

The following table shows the attribute values that Configuration Manager supports for the client certificate selection criteria.

OID ATTRIBUTE	DISTINGUISHED NAME ATTRIBUTE	ATTRIBUTE DEFINITION
0.9.2342.19200300.100.1.25	DC	Domain component
1.2.840.113549.1.9.1	E or E-mail	Email address
2.5.4.3	CN	Common name
2.5.4.4	SN	Subject name
2.5.4.5	SERIALNUMBER	Serial number
2.5.4.6	C	Country code
2.5.4.7	L	Locality
2.5.4.8	S or ST	State or province name
2.5.4.9	STREET	Street address
2.5.4.10	O	Organization name
2.5.4.11	OU	Organizational unit
2.5.4.12	T or Title	Title

OID ATTRIBUTE	DISTINGUISHED NAME ATTRIBUTE	ATTRIBUTE DEFINITION
2.5.4.42	G or GN or GivenName	Given name
2.5.4.43	I or Initials	Initials
2.5.29.17	(no value)	Subject Alternative Name

If more than one appropriate certificate is located after the selection criteria are applied, you can override the default configuration to select the certificate that has the longest validity period and instead, specify that no certificate is selected. In this scenario, the client won't be able to communicate with IIS site systems with a PKI certificate. The client sends an error message to its assigned fallback status point to alert you to the certificate selection failure so that you can change or refine your certificate selection criteria. The client behavior then depends on whether the failed connection was over HTTPS or HTTP:

- If the failed connection was over HTTPS: The client tries to connect over HTTP and uses the client self-signed certificate.
- If the failed connection was over HTTP: The client tries to connect again over HTTP by using the self-signed client certificate.

To help identify a unique PKI client certificate, you can also specify a custom store other than the default of **Personal** in the **Computer** store. However, you must create this store independently from Configuration Manager. You must be able to deploy certificates to this custom store and renew them before the validity period expires.

For more information, see Configure settings for client PKI certificates.

Plan a transition strategy for PKI certificates and internet-based client management

The flexible configuration options in Configuration Manager let you gradually transition clients and the site to use PKI certificates to help secure client endpoints. PKI certificates provide better security and enable you to manage internet clients.

Because of the number of configuration options and choices in Configuration Manager, there's no single way to transition a site so that all clients use HTTPS connections. However, you can follow these steps as guidance:

1. Install the Configuration Manager site and configure it so that site systems accept client connections over HTTPS and HTTP.
2. Configure the **Client Computer Communication** tab in the site properties so that the **Site System Settings** is **HTTP or HTTPS**, and select **Use PKI client certificate (client authentication capability) when available**. For more information, see Configure settings for client PKI certificates.

   > **NOTE**
   > Starting in version 1906, this tab is called **Communication Security**.

3. Pilot a PKI rollout for client certificates. For an example deployment, see Deploy the client certificate for Windows computers.
4. Install clients by using the client push installation method. For more information, see the How to install Configuration Manager clients by using client push.
5. Monitor client deployment and status by using the reports and information in the Configuration Manager console.

6. Track how many clients are using a client PKI certificate by viewing the **Client Certificate** column in the **Assets and Compliance** workspace, **Devices** node.

   You can also deploy the Configuration Manager HTTPS Readiness Assessment Tool (**cmHttpsReadiness.exe**) to computers. Then use the reports to view how many computers can use a client PKI certificate with Configuration Manager.

   > **NOTE**
   > When you install the Configuration Manager client, it installs the **CMHttpsReadiness.exe** tool in the `%windir%\CCM` folder. The following command-line options are available when you run this tool:
   >
   > - `/Store:<name>`: This option is the same as the **CCMCERTSTORE** client.msi property
   > - `/Issuers:<list>`: This option is the same as the **CCMCERTISSUERS** client.msi property
   > - `/Criteria:<criteria>`: This option is the same as the **CCMCERTSEL** client.msi property
   > - `/SelectFirstCert`: This option is the same as the **CCMFIRSTCERT** client.msi property
   >
   > For more information, see About client installation properties.

7. When you're confident that enough clients are successfully using their client PKI certificate for authentication over HTTP, follow these steps:

   a. Deploy a PKI web server certificate to a member server that runs an additional management point for the site, and configure that certificate in IIS. For more information, see Deploy the web server certificate for site systems that run IIS.

   b. Install the management point role on this server and configure the **Client connections** option in the management point properties for **HTTPS**.

8. Monitor and verify that clients that have a PKI certificate use the new management point by using HTTPS. You can use IIS logging or performance counters to verify.

9. Reconfigure other site system roles to use HTTPS client connections. If you want to manage clients on the internet, make sure that site systems have an internet FQDN. Configure individual management points and distribution points to accept client connections from the internet.

   > **IMPORTANT**
   > Before you set up site system roles to accept connections from the internet, review the planning information and prerequisites for internet-based client management. For more information, see Communications between endpoints.

10. Extend the PKI certificate rollout for clients and for site systems that run IIS. Set up the site system roles for HTTPS client connections and internet connections, as required.

11. For the highest security: When you're confident that all clients are using a client PKI certificate for authentication and encryption, change the site properties to use HTTPS only.

    This plan first introduces PKI certificates for authentication only over HTTP, and then for authentication and encryption over HTTPS. When you follow this plan to gradually introduce these certificates, you reduce the risk that clients become unmanaged. You'll also benefit from the highest security that Configuration Manager supports.

Plan for the trusted root key

The Configuration Manager trusted root key provides a mechanism for Configuration Manager clients to verify

site systems belong to their hierarchy. Every site server generates a site exchange key to communicate with other sites. The site exchange key from the top-level site in the hierarchy is called the trusted root key.

The function of the trusted root key in Configuration Manager resembles a root certificate in a public key infrastructure. Anything signed by the private key of the trusted root key is trusted further down the hierarchy. Clients store a copy of the site's trusted root key in the **root\ccm\locationservices** WMI namespace.

For example, the site issues a certificate to the management point, which it signs with the private key of the trusted root key. The site shares with clients the public key of its trusted root key. Then clients can differentiate between management points that are in their hierarchy and management points that aren't in their hierarchy.

Clients automatically retrieve the public copy of the trusted root key by using two mechanisms:

- You extend the Active Directory schema for Configuration Manager, and publish the site to Active Directory Domain Services. Then clients retrieve this site information from a global catalog server. For more information, see Prepare Active Directory for site publishing.
- When you install clients using the client push installation method. For more information, see Client push installation.

If clients can't retrieve the trusted root key by using one of these mechanisms, they trust the trusted root key that's provided by the first management point that they communicate with. In this scenario, a client might be misdirected to an attacker's management point where it would receive policy from the rogue management point. This action requires a sophisticated attacker. This attack is limited to the short time before the client retrieves the trusted root key from a valid management point. To reduce this risk of an attacker misdirecting clients to a rogue management point, pre-provision the clients with the trusted root key.

Use the following procedures to pre-provision and verify the trusted root key for a Configuration Manager client:

- Pre-provision a client with the trusted root key by using a file
- Pre-provision a client with the trusted root key without using a file
- Verify the trusted root key on a client
- Remove or replace the trusted root key

> **NOTE**
>
> If clients can get the trusted root key from Active Directory Domain Services or client push, you don't have to pre-provision it.
>
> When clients use HTTPS communication to management points, you don't have to pre-provision the trusted root key. They establish trust by the PKI certificates.

Pre-provision a client with the trusted root key by using a file

1. On the site server, open the following file in a text editor:
   `<Configuration Manager install directory>\bin\mobileclient.tcf`
2. Locate the entry, **SMSPublicRootKey=**. Copy the key from that line, and close the file without any changes.
3. Create a new text file, and paste the key information that you copied from the mobileclient.tcf file.
4. Save the file in a location where all computers can access it, but where the file is safe from tampering.
5. Install the client by using any installation method that accepts client.msi properties. Specify the following property: `SMSROOTKEYPATH=<full path and file name>`

> **IMPORTANT**
> When you specify the trusted root key during client installation, also specify the site code. Use the following client.msi property: `SMSSITECODE=<site code>`

Pre-provision a client with the trusted root key without using a file

1. On the site server, open the following file in a text editor:
   `<Configuration Manager install directory>\bin\mobileclient.tcf`
2. Locate the entry, **SMSPublicRootKey=**. Copy the key from that line, and close the file without any changes.
3. Install the client by using any installation method that accepts client.msi properties. Specify the following client.msi property: `SMSPublicRootKey=<key>` where `<key>` is the string that you copied from mobileclient.tcf.

> **IMPORTANT**
> When you specify the trusted root key during client installation, also specify the site code. Use the following client.msi property: `SMSSITECODE=<site code>`

Verify the trusted root key on a client

1. Open a Windows PowerShell console as an administrator.
2. Run the following command:

```
(Get-WmiObject -Namespace root\ccm\locationservices -Class TrustedRootKey).TrustedRootKey
```

The returned string is the trusted root key. Verify that it matches the **SMSPublicRootKey** value in the mobileclient.tcf file on the site server.

Remove or replace the trusted root key

Remove the trusted root key from a client by using the client.msi property, **RESETKEYINFORMATION = TRUE**.

To replace the trusted root key, reinstall the client together with the new trusted root key. For example, use client push, or specify the client.msi property **SMSPublicRootKey**.

For more information on these installation properties, see About client installation parameters and properties.

Plan for signing and encryption

When you use PKI certificates for all client communications, you don't have to plan for signing and encryption to help secure client data communication. If you set up any site systems that run IIS to allow HTTP client connections, decide how to help secure the client communication for the site.

To help protect the data that clients send to management points, you can require clients to sign the data. You can also require the SHA-256 algorithm for signing. This configuration is more secure, but don't require SHA-256 unless all clients support it. Many operating systems natively support this algorithm, but older operating systems might require an update or hotfix.

While signing helps protect the data from tampering, encryption helps protect the data from information disclosure. You can enable 3DES encryption for the inventory data and state messages that clients send to management points in the site. You don't have to install any updates on clients to support this option. Clients and management points require additional CPU usage for encryption and decryption.

For more information about how to configure the settings for signing and encryption, see Configure signing and encryption.

Plan for role-based administration

For more information, see Fundamentals of role-based administration.

Plan for Azure Active Directory

Configuration Manager integrates with Azure Active Directory (Azure AD) to enable the site and clients to use modern authentication. Onboarding your site with Azure AD supports the following Configuration Manager scenarios:

Client

- Manage clients on the internet via cloud management gateway
- Manage cloud domain-joined devices
- Co-management
- Deploy user-available apps
- Microsoft Store for Business online apps
- Reduce infrastructure requirements. For example, Software Center using the management point instead of the application catalog
- Manage Office 365 apps

Server

- Upgrade Readiness
- Windows Analytics
- Azure Log Analytics
- Community Hub
- Cloud distribution point
- User discovery

For more information on connecting your site to Azure AD, see Configure Azure services.

For more information about Azure AD, see Azure Active Directory documentation.

Plan for SMS Provider authentication

Starting in version 1810, you can specify the minimum authentication level for administrators to access Configuration Manager sites. This feature enforces administrators to sign in to Windows with the required level. It applies to all components that access the SMS Provider. For example, the Configuration Manager console, SDK methods, and Windows PowerShell cmdlets.

This configuration is a hierarchy-wide setting. Before you change this setting, make sure that all Configuration Manager administrators can sign in to Windows with the required authentication level.

The following levels are available:

- **Windows authentication**: Require authentication with Active Directory domain credentials.

- **Certificate authentication**: Require authentication with a valid certificate that's issued by a trusted PKI certificate authority.
- **Windows Hello for Business authentication**: Require authentication with strong two-factor authentication that's tied to a device and uses biometrics or a PIN.

For more information, see Plan for the SMS Provider.

See also

- Security and privacy for Configuration Manager clients
- Configure security
- Communication between endpoints
- Cryptographic controls technical reference
- PKI certificate requirements

Security best practices and privacy information for System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the following information to find security best practices and privacy information for System Center Configuration Manager.

Security and privacy content:

- Security and privacy for site administration in System Center Configuration Manager
- Security and privacy for reporting in System Center Configuration Manager
- Security and privacy for migration to System Center Configuration Manager
- Security and privacy for clients in System Center Configuration Manager
- Security and privacy for content management for System Center Configuration Manager
- Security and privacy for application management in System Center Configuration Manager
- Security and privacy for software updates in System Center Configuration Manager
- Security and privacy for operating system deployment in System Center Configuration Manager
- Security and privacy for collections in System Center Configuration Manager
- Security and privacy for queries in System Center Configuration Manager
- Security and privacy for hardware inventory in System Center Configuration Manager
- Security and privacy for software inventory in System Center Configuration Manager
- Security and privacy for Asset Intelligence in System Center Configuration Manager
- Security and privacy for power management in System Center Configuration Manager
- Security and privacy for remote control in System Center Configuration Manager
- Security and privacy for software inventory in System Center Configuration Manager
- Security and privacy for compliance settings in System Center Configuration Manager
- See the *Security and privacy considerations for remote connection profiles* section in Remote connection profiles in System Center Configuration Manager
- Security and privacy for certificate profiles in System Center Configuration Manager
- Wi-Fi and VPN profile security and privacy in System Center Configuration Manager

Configuration Manager cmdlet library privacy statement

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This privacy statement covers the features for the System Center Configuration Manager Cmdlet Library.

Usage data

What this feature does

The System Center Configuration Manager cmdlet library lets you manage a Configuration Manager hierarchy by using Windows PowerShell cmdlets and scripts. The cmdlet library collects information about how you use the cmdlets in the library to identify trends and usage patterns. The cmdlet library also collects the types and numbers of errors that you receive when you use the cmdlets.

Information collected, processed, or transmitted

The collected usage data includes starting, stopping, and terminating of cmdlets, running of deprecated cmdlets, and activity metrics for SMS Provider operations that are related to the cmdlets. This information isn't personally identifiable. Collected error information includes errors that cmdlets return and error details for exception errors. Some error detail reports might inadvertently include individual identifiers, like a serial number for a device that is connected to your computer. The cmdlet library filters and anonymizes information that's in the error reports to remove individual identifiers before transmission to Microsoft.

Use of information

Microsoft uses this information to improve the quality, security, and integrity of the products and services they offer.

Choice/control

This usage data feature is enabled by default. The System Center Configuration Manager cmdlet library has two registry keys that control this functionality.

To fully opt out, set these two registry key values. They are for each of the Event Tracing for Windows (ETW) providers:

- HKLM\Software\Microsoft\ConfigMgr10\PowerShell\Microsoft.ConfigurationManagement.PowerShell.Provider:CeipLevel=0 (opts out of usage data for the drive provider)
- HKLM\Software\Microsoft\ConfigMgr10\PowerShell\Microsoft.ConfigurationManagement.PowerShell.Cmdlets:CeipLevel=0 (opts out of usage data for the cmdlets)

  Changes to the usage data settings are specific to the computer where they're made.

Next steps

System Center Configuration Manager Cmdlet Library documentation.

Additional information about privacy for Configuration Manager

2/12/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Updates and servicing

Configuration Manager uses an update model that helps keep your environment current with the latest updates and features. This feature uses a site system role called the service connection point. You choose the server where to install this role.

For more information about collected information and how it's used, see Usage data.

Usage data

Configuration Manager collects diagnostics and usage data about itself, which Microsoft uses to improve the installation experience, quality, and security of future releases. Diagnostics and usage data is enabled for each Configuration Manager hierarchy. It consists of SQL Server queries that run on a weekly basis on each primary site and at the central administration site. When the hierarchy uses a central administration site, the data from primary sites is then replicated to that site. At the top-level site of your hierarchy, the service connection point submits this information when it checks for updates. If the service connection point is in offline mode, the information is transferred by using the service connection tool.

Configuration Manager collects data only from the site's SQL server database, and it doesn't collect data directly from clients or site servers.

Administrators can change the level of data that's collected by going to the **Usage Data** section of the Configuration Manager console.

For more information about usage data levels and settings, see Diagnostics and usage data.

Customer Experience Improvement Program

> **NOTE**
> Starting in Configuration Manager version 1802, the CEIP feature is removed from the product.

The Customer Experience Improvement Program (CEIP) collects basic information from the Configuration Manager console about your hardware configuration and how you use our software and services to identify trends and usage patterns. CEIP also collects the type and number of errors that you encounter, software and hardware performance, and the speed of services. We don't collect your name, address, or other contact information. No CEIP data is collected from client computers.

We use this information to improve the quality, reliability, and performance of Microsoft software and services.

For more about the information that's collected, processed, or transmitted by CEIP, see the CEIP privacy statement.

Log Analytics Connector

The Log Analytics Connector syncs data, such as collections, from Configuration Manager to the Azure cloud service. The Azure subscription ID and secret key are stored in the Configuration Manager database when an admin configures the feature. Both the Azure Active Directory client secret and the Azure workspace shared key are stored in the on-premises Configuration Manager database. All communications between Configuration Manager and Azure use HTTPS. No additional information about the collections is provided to Microsoft outside of randomized diagnostics and usage data.

For more information about the information that Log Analytics collects, see Log analytics data security.

Asset Intelligence

Asset Intelligence lets administrators define, track, and proactively manage conformity with configuration standards. Metering and reporting on the deployment and use of both physical and virtual applications helps organizations make better business decisions about software licensing and maintain compliance with licensing agreements. After collecting usage data from Configuration Manager clients, you can use different features to view the data, including collections, queries, and reporting.

During each synchronization, a catalog of known software is downloaded from Microsoft. You can choose to send Microsoft information about uncategorized software titles that are discovered within your organization to be researched and added to the catalog. Prior to uploading this information, a dialog box shows data that's going to be uploaded. Uploaded data can't be recalled. Asset Intelligence doesn't send information about users and computers or license usage to Microsoft.

After a software title is uploaded, Microsoft researchers identify, categorize, and then make that knowledge available to all other customers who use this feature and other consumers of the catalog. Any uploaded software title becomes public. The application and its categorization become part of the catalog and then can be downloaded to other consumers of the catalog. Before you configure Asset Intelligence data collection and decide whether to submit information to Microsoft, consider the privacy requirements of your organization.

Asset Intelligence isn't enabled by default in Configuration Manager. Uploading uncategorized titles never occurs automatically, and the system isn't designed to automate this task. You must manually select and approve the upload of each software title.

Endpoint Protection

Microsoft Cloud Protection Service was formerly known as Microsoft Active Protection Service or MAPS.

The applicable products are System Center Endpoint Protection and the Endpoint Protection feature of System Center Configuration Manager (to manage System Center Endpoint Protection and Windows Defender for Windows 10). This feature isn't implemented for System Center Endpoint Protection for Linux or System Center Endpoint Protection for Mac.

The Microsoft Cloud Protection Service antimalware community is a voluntary worldwide online community that includes System Center Endpoint Protection users. When you join Microsoft Cloud Protection Service, System Center Endpoint Protection automatically sends information to Microsoft. Microsoft uses the information to determine software to investigate for potential threats and to help improve the effectiveness of System Center Endpoint Protection. This community helps stop the spread of new malicious software infections. If a Microsoft Cloud Protection Service report includes details about malware or potentially unwanted software that the Endpoint Protection client may be able to remove, Microsoft Cloud Protection Service downloads the latest signature to address it. Microsoft Cloud Protection Service can also find "false positives" and fix them. (False positives are where something originally identified as malware turns out not to be.)

Microsoft Cloud Protection Service reports include information about potential malware files, like file names, cryptographic hash, vendor, size, and date stamps. In addition, Microsoft Cloud Protection Service might collect full URLs to indicate the origin of the file. These URLs might occasionally have personal information like search terms

or data that was entered in forms. Reports might also include actions that you took when Endpoint Protection notified you about unwanted software. Microsoft Cloud Protection Service reports include this information to help Microsoft gauge how effectively Endpoint Protection can detect and remove malware and potentially unwanted software and to attempt to identify new malware.

You can join Microsoft Cloud Protection Service if you have a basic or advanced membership. Basic member reports have the information described previously. Advanced member reports are more comprehensive and may include additional details about the software that Endpoint Protection detects, like the location of such software, file names, how the software operates, and how it has affected your computer. These reports and reports from other Endpoint Protection users who participate in Microsoft Cloud Protection Service help Microsoft researchers discover new threats more rapidly. Malware definitions are then created for programs that meet the analysis criteria, and the updated definitions are made available to all users through Microsoft Update.

To help detect and fix certain kinds of malware infections, the product regularly sends Microsoft Cloud Protection Service information about the security state of your PC. This information includes information about your PC's security settings and log files that describe the drivers and other software that load while your PC boots.

A number that uniquely identifies your PC is also sent. Also, Microsoft Cloud Protection Service may collect the IP addresses that the potential malware files connect to.

Microsoft Cloud Protection Service reports are used to improve Microsoft software and services. The reports might also be used for statistical or other testing or analytical purposes and to generate definitions. Only Microsoft employees, contractors, partners, and vendors who have a business need to use the reports can access them.

Microsoft Cloud Protection Service does not intentionally collect personal information. To the extent that Microsoft Cloud Protection Service collects any personal information, Microsoft does not use the information to identify you or contact you.

For more information, see Endpoint Protection.

Site Hierarchy – Geographical View with Bing Maps

In the Configuration Manager console, go to the **Monitoring** workspace, select the **Site Hierarchy** node, and switch to the **Geographical View**. This view lets you use maps that Microsoft Bing Maps provides to view your Configuration Manager physical server topology. To enable this feature, location information that you provide is sent from your server to the Bing Maps Web service.

Microsoft uses the information to operate and improve Microsoft Bing Maps and other Microsoft sites and services. For more information, see the Microsoft Privacy Statement.

You can choose not to use the Geographical View for the Site Hierarchy. The default Hierarchy Diagram view lets you see the hierarchy and doesn't use the Bing Maps service.

Microsoft Intune subscription

Customers who bought a subscription to Microsoft Intune can use Configuration Manager to manage their mobile devices that are connected through Microsoft Intune. Microsoft Online Services Privacy Statement applies to the Microsoft online services, which includes Microsoft Intune. If customers also have a Microsoft Intune subscription, the Microsoft Online Services Privacy Statement should be read in conjunction with this privacy statement.

All communications with Microsoft Intune use HTTPS. To configure the Microsoft Intune subscription and to download the Certificate Signing Request (CSR) that's needed to configure iOS support, an admin must sign in to Microsoft Intune by using work account and password. These credentials aren't stored within Configuration Manager. All other communications with Microsoft Intune are authenticated by using PKI certificates that Microsoft Intune automatically generates.

To manage devices that are connected to Microsoft Intune, some information is sent to and received from

Microsoft Intune. This information includes the User Principal Name (UPN) of all users who are assigned to the service and device inventory information for those devices that are managed by Microsoft Intune. Metadata, like application name, publisher, and version, for content that is assigned to Manage.Microsoft.com distribution points is sent to Microsoft Intune. The actual binary content that's assigned to a Manage.Microsoft.com distribution point is encrypted before it is uploaded to Microsoft Intune.

This feature isn't configured by default. Admins control the content that is transferred to the Manage.Microsoft.com distribution point and the users who are assigned to the service. The feature can be removed at any time.

Configure security in Configuration Manager

7/26/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the information in this article to help you set up security-related options for Configuration Manager. It covers the following security options:

- Client computer communication for client PKI certificates
- Signing and encryption
- Role-based administration
- Manage accounts
- Configure Azure Active Directory
- Configure SMS Provider authentication

Configure settings for client PKI certificates

If you want to use public key infrastructure (PKI) certificates for client connections to site systems that use Internet Information Services (IIS), use the following procedure to configure settings for these certificates.

To configure client PKI certificate settings

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. Select the primary site to configure.
2. In the ribbon, choose **Properties**. Then switch to the **Client Computer Communication** tab.

   > **NOTE**
   > Starting in version 1906, this tab is called **Communication Security**.

3. Select the settings for site systems that use IIS.

   - **HTTPS only**: Clients that are assigned to the site always use a client PKI certificate when they connect to site systems that use IIS.
   - **HTTPS or HTTP**: You don't require clients to use PKI certificates.
   - **Use Configuration Manager-generated certificates for HTTP site systems**: For more information on this setting, see Enhanced HTTP.

4. Select the settings for client computers.

   - **Use client PKI certificate (client authentication capability) when available**: If you chose the **HTTPS or HTTP** site server setting, choose this option to use a client PKI certificate for HTTP connections. The client uses this certificate instead of a self-signed certificate to authenticate itself to site systems. If you chose **HTTPS only**, this option is automatically chosen.

   When more than one valid PKI client certificate is available on a client, choose **Modify** to configure the client certificate selection methods.

   For more information about the client certificate selection method, see Planning for PKI client certificate selection.

   - **Clients check the certificate revocation list (CRL) for site systems**: Enable this setting for clients to

check your organization's CRL for revoked certificates.

For more information about CRL checking for clients, see Planning for PKI certificate revocation.

5. To import, view, and delete the certificates for trusted root certification authorities, choose **Set**.

   For more information, see Planning for the PKI trusted root certificates and the certificate issuers List.

Repeat this procedure for all primary sites in the hierarchy.

Configure signing and encryption

Configure the most secure signing and encryption settings for site systems that all clients in the site can support. These settings are especially important when you let clients communicate with site systems by using self-signed certificates over HTTP.

To configure signing and encryption for a site

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. Select the primary site to configure.
2. In the ribbon, select **Properties**, and then switch to the **Signing and Encryption** tab.

   This tab is available on a primary site only. If you don't see the **Signing and Encryption** tab, make sure that you're not connected to a central administration site or a secondary site.
3. Configure the signing and encryption options for clients to communicate with the site.

   - **Require signing**: Clients sign data before sending to the management point.
   - **Require SHA-256**: Clients use the SHA-256 algorithm when signing data.

   > **WARNING**
   > Don't **Require SHA-256** without first confirming that all clients support this hash algorithm. These clients include ones that might be assigned to the site in the future.
   >
   > If you choose this option, and clients with self-signed certificates can't support SHA-256, Configuration Manager rejects them. The SMS_MP_CONTROL_MANAGER component logs the message ID 5443.

   - **Use encryption**: Clients encrypt client inventory data and status messages before sending to the management point. They use the 3DES algorithm.

Repeat this procedure for all primary sites in the hierarchy.

Configure role-based administration

Role-based administration combines security roles, security scopes, and assigned collections to define the administrative scope for each administrative user. A scope includes the objects that a user can view in the console, and the tasks related to those objects that they have permission to do. Role-based administration configurations are applied at each site in a hierarchy.

For more information, see Configure role-based administration. This article details the following actions:

- Create custom security roles
- Configure security roles
- Configure security scopes for an object
- Configure collections to manage security

- Create a new administrative user
- Modify the administrative scope of an administrative user

> **IMPORTANT**
> Your own administrative scope defines the objects and settings that you can assign when you configure role-based administration for another administrative user. For information about planning for role-based administration, see Fundamentals of role-based administration.

Manage accounts that Configuration Manager uses

Configuration Manager supports Windows accounts for many different tasks and uses. To view accounts that are configured for different tasks, and to manage the password that Configuration Manager uses for each account, use the following procedure:

To manage accounts that Configuration Manager uses

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Security**, and then choose the **Accounts** node.
2. To change the password for an account, select the account in the list. Then choose **Properties** in the ribbon.
3. Choose **Set** to open the **Windows User Account** dialog box. Specify the new password for Configuration Manager to use for this account.

   > **NOTE**
   > The password that you specify must match this account's password in Active Directory.

For more information, see Accounts used in Configuration Manager.

Configure Azure Active Directory

Integrate Configuration Manager with Azure Active Directory (Azure AD) to simplify and cloud-enable your environment. Enable the site and clients to authenticate by using Azure AD. For more information, see the **Cloud Management** service in Configure Azure services.

Configure SMS Provider authentication

Starting in version 1810, you can specify the minimum authentication level for administrators to access Configuration Manager sites. This feature enforces administrators to sign in to Windows with the required level. For more information, see Plan for the SMS Provider.

See also

- Plan for security
- Security and privacy for Configuration Manager clients
- Communication between endpoints
- Cryptographic controls technical reference
- PKI certificate requirements

Cryptographic controls technical reference

9/11/2019 • 20 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

System Center Configuration Manager uses signing and encryption to help protect the management of the devices in the Configuration Manager hierarchy. With signing, if data has been altered in transit, it's discarded. Encryption helps prevent an attacker from reading the data by using a network protocol analyzer.

The primary hashing algorithm that Configuration Manager uses for signing is SHA-256. When two Configuration Manager sites communicate with each other, they sign their communications with SHA-256. The primary encryption algorithm implemented in Configuration Manager is 3DES. This is used for storing data in the Configuration Manager database and for client HTTP communication. When you use client communication over HTTPS, you can configure your public key infrastructure (PKI) to use RSA certificates with the maximum hashing algorithms and key lengths that are documented in PKI certificate requirements.

For most cryptographic operations for Windows-based operating systems, Configuration Manager uses SHA-2, 3DES and AES, and RSA algorithms from the Windows CryptoAPI library rsaenh.dll.

> **IMPORTANT**
> See information about recommended changes in response to SSL vulnerabilities in About SSL Vulnerabilities.

Cryptographic controls for Configuration Manager operations

Information in Configuration Manager can be signed and encrypted, whether or not you use PKI certificates with Configuration Manager.

Policy signing and encryption

Client policy assignments are signed by the self-signed site server signing certificate to help prevent the security risk of a compromised management point sending policies that have been tampered with. This is important if you are using Internet-based client management because this environment requires a management point that is exposed to Internet communication.

Policy is encrypted with 3DES when it contains sensitive data. Policy that contains sensitive data is sent to authorized clients only. Policy that does not have sensitive data is not encrypted.

When policy is stored on the clients, it is encrypted with Data Protection application programming interface (DPAPI).

Policy hashing

When Configuration Manager clients request policy, they first get a policy assignment so that they know which policies apply to them, and then they request only those policy bodies. Each policy assignment contains the calculated hash for the corresponding policy body. The client retrieves the applicable policy bodies and then calculates the hash on that body. If the hash on the downloaded policy body does not match the hash in the policy assignment, the client discards the policy body.

The hashing algorithm for policy is SHA-1 and SHA-256.

Content hashing

The distribution manager service on the site server hashes the content files for all packages. The policy provider

includes the hash in the software distribution policy. When the Configuration Manager client downloads the content, the client regenerates the hash locally and compares it to the one supplied in the policy. If the hashes match, the content has not been altered and the client installs it. If a single byte of the content has been altered, the hashes will not match and the software will not be installed. This check helps to ensure that the correct software is installed because the actual content is crosschecked with the policy.

The default hashing algorithm for content is SHA-256. To change this default, see the documentation for the Configuration Manager Software Development Kit (SDK).

Not all devices can support content hashing. The exceptions include:

- Windows clients when they stream App-V content.
- Windows Phone clients, though these clients verify the signature of an application that is signed by a trusted source.
- Windows RT client, though these clients verify the signature of an application that is signed by a trusted source and also use package full name (PFN) validation.
- iOS, though these devices verify the signature of an application that is signed by any developer certificate from a trusted source.
- Nokia client, though, these clients verify the signature of an application that uses a self-signed certificate. Or, the signature of a certificate from a trusted source and the certificate can sign Nokia Symbian Installation Source (SIS) applications.
- Android. In addition, these devices do not use signature validation for application installation.
- Clients that run on versions of Linux and UNIX that do not support SHA-256. For more information, see Planning for client deployment to Linux and UNIX computers.

Inventory signing and encryption

Inventory that clients send to management points is always signed by devices, regardless of whether they communicate with management points over HTTP or HTTPS. If they use HTTP, you can choose to encrypt this data, which is a security best practice.

State migration encryption

Data stored on state migration points for operating system deployment is always encrypted by the User State Migration Tool (USMT) by using 3DES.

Encryption for multicast packages to deploy operating systems

For every operating system deployment package, you can enable encryption when the package is transferred to computers by using multicast. The encryption uses Advanced Encryption Standard (AES). If you enable encryption, no additional certificate configuration is required. The multicast-enabled distribution point automatically generates symmetric keys for encrypting the package. Each package has a different encryption key. The key is stored on the multicast-enabled distribution point by using standard Windows APIs. When the client connects to the multicast session, the key exchange occurs over a channel encrypted with either the PKI-issued client authentication certificate (when the client uses HTTPS) or the self-signed certificate (when the client uses HTTP). The client stores the key in memory only for the duration of the multicast session.

Encryption for media to deploy operating systems

When you use media to deploy operating systems and specify a password to protect the media, the environment variables are encrypted by using Advanced Encryption Standard (AES). Other data on the media, including packages and content for applications, is not encrypted.

Encryption for content that is hosted on cloud-based distribution points

Beginning with System Center 2012 Configuration Manager SP1, when you use cloud-based distribution points,

the content that you upload to these distribution points is encrypted by using Advanced Encryption Standard (AES) with a 256-bit key size. The content is re-encrypted whenever you update it. When clients download the content, it is encrypted and protected by the HTTPS connection.

Signing in software updates

All software updates must be signed by a trusted publisher to protect against tampering. On client computers, the Windows Update Agent (WUA) scans for the updates from the catalog, but will not install the update if it cannot locate the digital certificate in the Trusted Publishers store on the local computer. If a self-signed certificate was used for publishing the updates catalog, such as WSUS Publishers Self-signed, the certificate must also be in the Trusted Root Certification Authorities certificate store on the local computer to verify the validity of the certificate. WUA also checks whether the **Allow signed content from intranet Microsoft update service location Group Policy** setting is enabled on the local computer. This policy setting must be enabled for WUA to scan for the updates that were created and published with Updates Publisher.

When software updates are published in System Center Updates Publisher, a digital certificate signs the software updates when they are published to an update server. You can either specify a PKI certificate or configure Updates Publisher to generate a self-signed certificate to sign the software update.

Signed configuration data for compliance settings

When you import configuration data, Configuration Manager verifies the file's digital signature. If the files have not been signed, or if the digital signature verification check fails, you will be warned and prompted whether to continue with the import. Continue to import the configuration data only if you explicitly trust the publisher and the integrity of the files.

Encryption and hashing for client notification

If you use client notification, all communication uses TLS and the highest encryption that the server and client operating systems can negotiate. For example, a client computer running Windows 7 and a management point running Windows Server 2008 R2 can support 128-bit AES encryption, whereas a client computer running Vista to the same management point will negotiate down to 3DES encryption. The same negotiation occurs for hashing the packets that are transferred during client notification, which uses SHA-1 or SHA-2.

Certificates used by Configuration Manager

For a list of the public key infrastructure (PKI) certificates that can be used by Configuration Manager, any special requirements or limitations, and how the certificates are used, see PKI certificate requirements. This list includes the supported hash algorithms and key lengths. Most certificates support SHA-256 and 2048 bits key length.

> **NOTE**
> All certificates that Configuration Manager uses must contain only single-byte characters in the subject name or subject alternative name.

PKI certificates are required for the following scenarios:

- When you manage Configuration Manager clients on the Internet.
- When you manage Configuration Manager clients on mobile devices.
- When you manage Mac computers.
- When you use cloud-based distribution points.

  For most other Configuration Manager communications that require certificates for authentication, signing, or encryption, Configuration Manager automatically uses PKI certificates if they are available. If they are not available, Configuration Manager generates self-signed certificates.

Configuration Manager does not use PKI certificates when it manages mobile devices by using the Exchange Server connector.

Mobile device management and PKI certificates

If the mobile device has not been locked by the mobile operator, you can use Configuration Manager or Microsoft Intune to request and install a client certificate. This certificate provides mutual authentication between the client on the mobile device and Configuration Manager site systems or Microsoft Intune services. If your mobile device is locked, you cannot use Configuration Manager or Intune to deploy certificates.

If you enable hardware inventory for mobile devices, Configuration Manager or Intune also inventories the certificates that are installed on the mobile device.

Operating system deployment and PKI certificates

When you use Configuration Manager to deploy operating systems and a management point requires HTTPS client connections, the client computer must also have a certificate to communicate with the management point, even though it is in a transitional phase such as booting from task sequence media or a PXE-enabled distribution point. To support this scenario, you must create a PKI client authentication certificate and export it with the private key and then import it to the site server properties and also add the management point's trusted root CA certificate.

If you create bootable media, you import the client authentication certificate when you create the bootable media. Configure a password on the bootable media to help protect the private key and other sensitive data configured in the task sequence. Every computer that boots from the bootable media will present the same certificate to the management point as required for client functions such as requesting client policy.

If you use PXE boot, you import the client authentication certificate to the PXE-enabled distribution point and it uses the same certificate for every client that boots from that PXE-enabled distribution point. As a security best practice, require users who connect their computers to a PXE service to supply a password to help protect the private key and other sensitive data in the task sequences.

If either of these client authentication certificates is compromised, block the certificates in the **Certificates** node in the **Administration** workspace, **Security** node. To manage these certificates, you must have the **Manage operating system deployment certificate** right.

After the operating system is deployed and the Configuration Manager is installed, the client will require its own PKI client authentication certificate for HTTPS client communication.

ISV proxy solutions and PKI certificates

Independent Software Vendors (ISVs) can create applications that extend Configuration Manager. For example, an ISV could create extensions to support non-Windows client platforms such as Macintosh or UNIX computers. However, if the site systems require HTTPS client connections, these clients must also use PKI certificates for communication with the site. Configuration Manager includes the ability to assign a certificate to the ISV proxy that enables communications between the ISV proxy clients and the management point. If you use extensions that require ISV proxy certificates, consult the documentation for that product. For more information about how to create ISV proxy certificates, see the Configuration Manager Software Developer Kit (SDK).

If the ISV certificate is compromised, block the certificate in the **Certificates** node in the **Administration** workspace, **Security** node.

Asset intelligence and certificates

Configuration Manager installs with an X.509 certificate that the Asset Intelligence synchronization point uses to connect to Microsoft. Configuration Manager uses this certificate to request a client authentication certificate from the Microsoft certificate service. The client authentication certificate is installed on the Asset Intelligence synchronization point site system server and it is used to authenticate the server to Microsoft. Configuration Manager uses the client authentication certificate to download the Asset Intelligence catalog and to upload software titles.

This certificate has a key length of 1024 bits.

Cloud-based distribution points and certificates

Beginning with System Center 2012 Configuration Manager SP1, cloud-based distribution points require a management certificate (self-signed or PKI) that you upload to Microsoft Azure. This management certificate requires server authentication capability and a certificate key length of 2048 bits. In addition, you must configure a service certificate for each cloud-based distribution point, which cannot be self-signed but also has server authentication capability and a minimum certificate key length of 2048 bits.

> **NOTE**
>
> The self-signed management certificate is for testing purposes only and not for use on production networks.

Clients do not require a client PKI certificate to use cloud-based distribution points; they authenticate to the management by using either a self-signed certificate or a client PKI certificate. The management point then issues a Configuration Manager access token to the client, which the client presents to the cloud-based distribution point. The token is valid for 8 hours.

The Microsoft Intune Connector and certificates

When Microsoft Intune enrolls mobile devices, you can manage these mobile devices in Configuration Manager by creating a Microsoft Intune connector. The connector uses a PKI certificate with client authentication capability to authenticate Configuration Manager to Microsoft Intune and to transfer all information between them by using SSL. The certificate key size is 2048 bits and uses the SHA-1 hash algorithm.

When you install the connector, a signing certificate is created and stored on the site server for sideloading keys, and an encryption certificate is created and stored on the certificate registration point to encrypt the Simple Certificate Enrollment Protocol (SCEP) challenge. These certificates also have a key size of 2048 bits and use the SHA-1 hash algorithm.

When Intune enrolls mobile devices, it installs a PKI certificate onto the mobile device. This certificate has client authentication capability, uses a key size of 2048 bits, and uses the SHA-1 hash algorithm.

These PKI certificates are automatically requested, generated, and installed by Microsoft Intune.

CRL checking for PKI certificates

A PKI certificate revocation list (CRL) increases administrative and processing overhead but it is more secure. However, if CRL checking is enabled but the CRL is inaccessible, the PKI connection fails. For more information, see Security and privacy for Configuration Manager.

Certificate revocation list (CRL) checking is enabled by default in IIS, so if you are using a CRL with your PKI deployment, there is nothing additional to configure on most Configuration Manager site systems that run IIS. The exception is for software updates, which requires a manual step to enable CRL checking to verify the signatures on software update files.

CRL checking is enabled by default for client computers when they use HTTPS client connections. You cannot disable CRL checking for clients on Mac computers in Configuration Manager SP1 or later.

CRL checking is not supported for the following connections in Configuration Manager:

- Server-to-server connections.
- Mobile devices that are enrolled by Configuration Manager.
- Mobile devices that are enrolled by Microsoft Intune.

Cryptographic controls for server communication

Configuration Manager uses the following cryptographic controls for server communication.

Server communication within a site

Each site system server uses a certificate to transfer data to other site systems in the same Configuration Manager site. Some site system roles also use certificates for authentication. For example, if you install the enrollment proxy point on one server and the enrollment point on another server, they can authenticate one another by using this identity certificate. When Configuration Manager uses a certificate for this communication, if there is a PKI certificate available that has server authentication capability, Configuration Manager automatically uses it; if not, Configuration Manager generates a self-signed certificate. This self-signed certificate has server authentication capability, uses SHA-256, and has a key length of 2048 bits. Configuration Manager copies the certificate to the Trusted People store on other site system servers that might need to trust the site system. Site systems can then trust one another by using these certificates and PeerTrust.

In addition to this certificate for each site system server, Configuration Manager generates a self-signed certificate for most site system roles. When there is more than one instance of the site system role in the same site, they share the same certificate. For example, you might have multiple management points or multiple enrollment points in the same site. This self-signed certificate also uses SHA-256 and has a key length of 2048 bits. It is also copied to the Trusted People Store on site system servers that might need to trust it. The following site system roles generate this certificate:

- Application Catalog web service point
- Application Catalog website point
- Asset Intelligence synchronization point
- Certificate registration point
- Endpoint Protection point
- Enrollment point
- Fallback status point
- Management point
- Multicast-enabled distribution point
- Reporting services point
- Software update point
- State migration point
- Microsoft Intune connector

These certificates are managed automatically by Configuration Manager, and where necessary, automatically generated.

Configuration Manager also uses a client authentication certificate to send status messages from the distribution point to the management point. When the management point is configured for HTTPS client connections only, you must use a PKI certificate. If the management point accepts HTTP connections, you can use a PKI certificate or select the option to use a self-signed certificate that has client authentication capability, uses SHA-256, and has a key length of 2048 bits.

Server communication between sites

Configuration Manager transfers data between sites by using database replication and file-based replication. For

more information, see Communications between endpoints.

Configuration Manager automatically configures the database replication between sites and uses PKI certificates that have server authentication capability if these are available; if not, Configuration Manager creates self-signed certificates for server authentication. In both cases, authentication between sites is established by using certificates in the Trusted People Store that uses PeerTrust. This certificate store is used to ensure that only the SQL Server computers that are used by the Configuration Manager hierarchy participate in site-to-site replication. Whereas primary sites and the central administration site can replicate configuration changes to all sites in the hierarchy, secondary sites can replicate configuration changes only to their parent site.

Site servers establish site-to-site communication by using a secure key exchange that happens automatically. The sending site server generates a hash and signs it with its private key. The receiving site server checks the signature by using the public key and compares the hash with a locally generated value. If they match, the receiving site accepts the replicated data. If the values do not match, Configuration Manager rejects the replication data.

Database replication in Configuration Manager uses the SQL Server Service Broker to transfer data between sites by using the following mechanisms:

- SQL Server to SQL Server connection: This uses Windows credentials for server authentication and self-signed certificates with 1024 bits to sign and encrypt the data by using Advanced Encryption Standard (AES). If PKI certificates with server authentication capability are available, these will be used. The certificate must be located in the Personal store for the Computer certificate store.
- SQL Service Broker: This uses self-signed certificates with 2048 bits for authentication and to sign and encrypt the data by using Advanced Encryption Standard (AES). The certificate must be located in the SQL Server master database.

  File-based replication uses the Server Message Block (SMB) protocol, and uses SHA-256 to sign this data that is not encrypted but does not contain any sensitive data. If you want to encrypt this data, you can use IPsec and must implement this independently from Configuration Manager.

Cryptographic controls for clients that use HTTPS communication to site systems

When site system roles accept client connections, you can configure them to accept HTTPS and HTTP connections, or only HTTPS connections. Site system roles that accept connections from the Internet only accept client connections over HTTPS.

Client connections over HTTPS offer a higher level of security by integrating with a public key infrastructure (PKI) to help protect client-to-server communication. However, configuring HTTPS client connections without a thorough understanding of PKI planning, deployment, and operations could still leave you vulnerable. For example, if you do not secure your root CA, attackers could compromise the trust of your entire PKI infrastructure. Failing to deploy and manage the PKI certificates by using controlled and secured processes might result in unmanaged clients that cannot receive critical software updates or packages.

> **IMPORTANT**
> The PKI certificates that are used for client communication protect the communication only between the client and some site systems. They do not protect the communication channel between the site server and site systems or between site servers.

Communication that is unencrypted when clients use HTTPS communication

When clients communicate with site systems by using HTTPS, communications are usually encrypted over SSL. However, in the following situations, clients communicate with site systems without using encryption:

- Client fails to make an HTTPS connection on the intranet and fall back to using HTTP when site systems

allow this configuration

- Communication to the following site system roles:
  - Client sends state messages to the fallback status point
  - Client sends PXE requests to a PXE-enabled distribution point
  - Client sends notification data to a management point

  Reporting services points are configured to use HTTP or HTTPS independently from the client communication mode.

Cryptographic controls for clients chat use HTTP communication to site systems

When clients use HTTP communication to site system roles, they can use PKI certificates for client authentication, or self-signed certificates that Configuration Manager generates. When Configuration Manager generates self-signed certificates, they have a custom object identifier for signing and encryption, and these certificates are used to uniquely identify the client. For all supported operating systems except Windows Server 2003, these self-signed certificates use SHA-256, and have a key length of 2048 bits. For Windows Server 2003, SHA1 is used with a key length of 1024 bits.

Operating system deployment and self-signed certificates

When you use Configuration Manager to deploy operating systems with self-signed certificates, a client computer must also have a certificate to communicate with the management point, even if the computer is in a transitional phase such as booting from task sequence media or a PXE-enabled distribution point. To support this scenario for HTTP client connections, Configuration Manager generates self-signed certificates that have a custom object identifier for signing and encryption, and these certificates are used to uniquely identify the client. For all supported operating systems except Windows Server 2003, these self-signed certificates use SHA-256, and have a key length of 2048 bits. For Windows Server 2003, SHA1 is used with a key length of 1024 bits. If these self-signed certificates are compromised, to prevent attackers from using them to impersonate trusted clients, block the certificates in the **Certificates** node in the **Administration** workspace, **Security** node.

Client and server authentication

When clients connect over HTTP, they authenticate the management points by using either Active Directory Domain Services or by using the Configuration Manager trusted root key. Clients do not authenticate other site system roles, such as state migration points or software update points.

When a management point first authenticates a client by using the self-signed client certificate, this mechanism provides minimal security because any computer can generate a self-signed certificate. In this scenario, the client identity process must be augmented by approval. Only trusted computers must be approved, either automatically by Configuration Manager, or manually, by an administrative user. For more information, see the approval section in Communications between endpoints.

About SSL vulnerabilities

To improve the security of your Configuration Manager clients and servers, do the following:

- Enable TLS 1.2

  To enable TLS 1.2 for Configuration Manager, see How to enable TLS 1.2 for Configuration Manager.

- Disable SSL 3.0, TLS 1.0, and TLS 1.1
- Reorder the TLS-related cipher suites

For more information, see How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll and Prioritizing Schannel Cipher Suites. These procedures do not affect Configuration Manager functionality.

How to enable TLS 1.2

9/11/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article describes how to enable TLS 1.2 for Configuration Manager, including for individual components. Update requirements for commonly used features, and troubleshooting of some common problems, are also described in this article.

Configuration Manager relies on many different components for secure communication. The protocol that's used for a given connection depends on the capabilities of all the required components. If one component is out-of-date, the communication might use an older, less secure protocol.

To correctly enable Configuration Manager to support TLS 1.2, first enable TLS 1.2 for all required components. The required components depend on your environment and the Configuration Manager features that you use.

Start this process with the clients, especially previous versions of Windows. Before you enable TLS 1.2 on the Configuration Manager servers, make sure that all clients support TLS 1.2. Otherwise, the clients won't be able to communicate with the servers and can be orphaned.

Tasks for features and scenarios

To enable TLS 1.2 for components that Configuration Manager depends on for secure communication, you must:

- Enable TLS 1.2 protocol as a security provider
- Update .NET Framework to support TLS 1.2
- Update SQL Server and client components
- Update Windows and WinHTTP on Windows 8.0, Windows Server 2012 R2 and earlier
- Update Windows Server Update Services (WSUS)

This section describes the dependencies for specific Configuration Manager features and scenarios. To determine the next steps, locate the items that apply to your environment.

FEATURE OR SCENARIO	UPDATE TASKS
Site servers (central, primary, or secondary)	- Update .NET Framework - Verify strong cryptography settings
Site database server	Update SQL Server and its client components
Secondary site servers	Update SQL Server and its client components to a compliant version of SQL Express
Site system roles	- Update .NET Framework and verify strong cryptography settings - Update SQL Server and its client components on roles that require it, including the SQL Server Native Client
Reporting services point	- Update .NET Framework on the site server, the SQL Reporting Services servers, and any computer with the console - Restart the SMS_Executive service as necessary

FEATURE OR SCENARIO	UPDATE TASKS
Software update point	Update WSUS
Cloud management gateway	Enforce TLS 1.2
Configuration Manager console	- Update .NET Framework - Verify strong cryptography settings
Configuration Manager client with HTTPS site system roles	Update Windows to support TLS 1.2 for client-server communications by using WinHTTP
Software Center	- Update .NET Framework - Verify strong cryptography settings
Windows 7 clients	*Before* you enable TLS 1.2 on any server components, update Windows to support TLS 1.2 for client-server communications by using WinHTTP. If you enable TLS 1.2 on server components first, you can orphan earlier versions of clients.

Enable TLS 1.2 protocol as a security provider

Verify the `\SecurityProviders\SCHANNEL\Protocols` registry subkey setting, as shown in Transport layer security (TLS) best practices with the .NET Framework.

> **NOTE**
> TLS 1.2 is enabled by default. Therefore, no change to these keys is required to enable it. You can make changes under Protocols to disable TLS 1.0 and TLS 1.1 after you have followed the rest of the guidance in this article, and you have verified that the environment works by having only TLS 1.2 enabled.

Update .NET Framework to support TLS 1.2

Determine .NET version

First, determine your .NET version number. For more information, see How to determine which versions and service pack levels of the Microsoft .NET Framework are installed.

Install .NET updates

Some versions of .NET Framework might require updates to enable strong cryptography. Use these guidelines:

- NET Framework 4.6.2 and later supports TLS 1.1 and TLS 1.2. Confirm the registry settings, but no additional changes are required.
- Update NET Framework 4.6 and earlier versions to support TLS 1.1 and TLS 1.2. For more information, see .NET Framework versions and dependencies.
- If you're using .NET Framework 4.5.1 or 4.5.2 on Windows 8.1 or Windows Server 2012, the relevant updates and details are also available from the Download Center.

Configure for strong cryptography

Configure .NET Framework to support strong cryptography. Set the `SchUseStrongCrypto` registry setting to `DWORD:00000001`. This value disables the RC4 stream cipher and requires a restart. For more information about this setting, see Microsoft Security Advisory 296038.

Make sure to set the following registry keys on any computer that communicates across the network with a TLS

1.2-enabled system. For example, Configuration Manager clients, or any remote site system role that's not installed on the site server.

For 32-bit applications that are running on 32-bit systems or 64-bit applications that are running on 64-bit systems, update the following subkey value:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
      "SystemDefaultTlsVersions" = dword:00000001
      "SchUseStrongCrypto" = dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
      "SystemDefaultTlsVersions" = dword:00000001
      "SchUseStrongCrypto" = dword:00000001
```

For 32-bit applications that are running on 64-bit systems, update the following subkey value:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727]
      "SystemDefaultTlsVersions" = dword:00000001
      "SchUseStrongCrypto" = dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319]
      "SystemDefaultTlsVersions" = dword:00000001
      "SchUseStrongCrypto" = dword:00000001
```

> **NOTE**
>
> The `SchUseStrongCrypto` setting allows .NET to use TLS 1.1 and TLS 1.2. The `SystemDefaultTlsVersions` setting allows .NET to use the OS configuration. For more information, see TLS best practices with the .NET Framework.

Update SQL Server and client components

Microsoft SQL Server 2016 and later support TLS 1.1 and TLS 1.2. Earlier versions and dependent libraries might require updates. For more information, see KB 3135244: TLS 1.2 support for Microsoft SQL Server.

Secondary site servers need to use at least SQL Server 2016 Express with Service Pack 2 (13.2.50.26) or later.

SQL Server Native Client

> **NOTE**
>
> KB 3135244 also describes requirements for SQL Server client components.

Make sure to also update the SQL Server Native Client to at least version SQL 2012 SP4 (11.*.7001.0). Starting in version 1810, this requirement is a prerequisite check (warning).

Configuration Manager uses SQL Server Native Client on the following site system roles:

- Site database server
- Site server: central administration site, primary site, or secondary site
- Management point
- Device management point
- State migration point
- SMS Provider
- Software update point
- Multicast-enabled distribution point
- Asset Intelligence update service point

- Reporting services point
- Application catalog web service
- Enrollment point
- Endpoint Protection point
- Service connection point
- Certificate registration point
- Data warehouse service point

Update Windows and WinHTTP

Windows 8.1, Windows Server 2012 R2, Windows 10, Windows Server 2016, and later versions of Windows natively support TLS 1.2 for client-server communications over WinHTTP.

Earlier versions of Windows, such as Windows 7 or Windows Server 2012, don't enable TLS 1.1 or 1.2 by default for client-server communications through HTTPS. For these earlier versions of Windows, install Update 3140245 to enable TLS 1.1 and TLS 1.2 as the default secure protocols for WinHTTP in Windows. Then set the following registry values:

> **IMPORTANT**
> Enable these settings on all clients *before* enabling TLS 1.2 on the Configuration Manager servers. Otherwise, you can inadvertently orphan them.

Verify the value of the `DefaultSecureProtocols` registry setting, for example:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\
      DefaultSecureProtocols = (DWORD): 0xAA0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\
      DefaultSecureProtocols = (DWORD): 0xAA0
```

If you change this value, restart the computer.

> **NOTE**
> The example above shows the value of `0xAA0` for the WinHTTP `DefaultSecureProtocols` setting. KB 3140245: Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows lists the hexidecimal value for each protocol. By default in Windows, this value is `0x0A0` to enable SSL 3.0 and TLS 1.0 for WinHTTP. The above example keeps these defaults, and also enables TLS 1.1 and TLS 1.2 for WinHTTP. This configuration ensures that the change doesn't break any other application that might still rely on SSL 3.0 or TLS 1.0. You can use the value of `0xA00` to only enable TLS 1.1 and TLS 1.2. Configuration Manager supports the most secure protocol that Windows negotiates between both devices.
>
> If you want to completely disable SSL 3.0 and TLS 1.0, use the SChannel disabled protocols setting in Windows. For more information, see How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll.

Update Windows Server Update Services (WSUS)

To support TLS 1.2 for client-server communications in WSUS on Windows Server 2012 and Windows Server 2012 R2, install the following update on the WSUS server:

- For WSUS server that's running Windows Server 2012, install update 4022721 or a later update.
- For WSUS server that's running Windows Server 2012 R2, install update 4022720 or a later update.

Known issues

This section provides advice for common issues that occur when you enable TLS 1.2 support.

Unsupported platforms

The following client platforms are supported by Configuration Manager but aren't supported in a TLS 1.2 environment:

- Windows Server 2008
- Windows CE
- Apple OS X
- Windows 10 devices managed with on-premises MDM

Reports don't show in the console

If reports don't show in the Configuration Manager console, make sure to update the computer on which you're running the console. You need to update the .NET Framework, and enable strong cryptography.

FIPS security policy enabled

If you enable the FIPS security policy setting for either the client or a server, Secure Channel (Schannel) negotiation can cause them to use TLS 1.0. This behavior happens even if you disable the protocol in the registry.

To investigate, enable Secure Channel event logging, and then review Schannel events in the system log. For more information, see How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll.

SQL Server communication failure

If SQL Server communication fails and returns an **SslSecurityError** error, verify the following settings:

- Update .NET Framework, and enable strong cryptography on each machine
- Update SQL Server on the host server
- Update SQL client components on all systems that communicate with SQL. For example, the site servers, SMS provider, and site role servers.

Configuration Manager client communication failures

If the Configuration Manager client doesn't communicate with site roles, verify that you updated Windows to support TLS 1.2 for client-server communication by using WinHTTP. Common site roles include distribution points, management points, and state migration points.

Reporting services point fails and returns an expected error

If the reporting services point doesn't configure reports, check the **SRSRP.log** for the following error entry:

```
The underlying connection was closed: An expected error occurred on a receive.
```

To resolve this issue, follow these steps:

1. Update .NET Framework, and enable strong cryptography on all relevant computers.
2. After you install any updates, restart the SMS_Executive service.

Application catalog doesn't initialize

> **IMPORTANT**
> The application catalog is deprecated. For more information, see Removed and deprecated features.

If the application catalog doesn't initialize, check the **ServicePortalWebSite.svclog** file for the following error entry:

```
SOAP security negotiation failed. The client and server can't communicate because they don't share a common algorithm.
```

To resolve this issue, follow these steps:

1. Update .NET Framework, and enable strong cryptography on all relevant computers.
2. In the `%WinDir%\System32\InetSrv` folder of the application catalog server, create a **W2SP.exe.config** file with the following contents:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <runtime>
  <AppContextSwitchOverrides
value="Switch.System.ServiceModel.DisableUsingServicePointManagerSecurityProtocols=false;Switch.System.N
et.DontEnableSchUseStrongCrypto=false" />
  </runtime>
</configuration>
```

> **NOTE**
> This file is the default file that's created if the application was built by using .NET Framework 4.6.3.

3. Use HTTPS transport security for application catalog roles.

> **IMPORTANT**
> When you use HTTP message security for application catalog roles, WCF is hard-coded to use SSL 3.0 and TLS 1.0 only. This prevents the use of TLS 1.2.

4. If you made any changes, restart the computer.

Software Center or browser doesn't communicate with the application catalog

> **IMPORTANT**
> The application catalog is deprecated. For more information, see Removed and deprecated features.

The best method to make Software Center work with for user-available apps in a TLS 1.2-enabled site, remove the application catalog role. Then let Software Center communicate directly with a management point. For more information, see Remove the application catalog.

If you need to resolve communication failures between the application catalog and Software Center, verify the following conditions:

- Update .NET Framework, and enable strong cryptography on each computer.
- After you make the changes, restart all affected computers.

Service connection point upload failures

If the service connection point doesn't upload data to SCCMConnectedService, update the .NET Framework, and enable strong cryptography on each computer. After you make the changes, remember to restart the computers.

Configuration Manager console displays Intune onboarding dialog box

If the Intune onboarding dialog box appears when the console tries to connect to the Intune portal, update the .NET Framework, and enable strong cryptography on each computer. After you make the changes, remember to restart the computers.

Configuration Manager console displays failure to sign in to Azure

When you try to create applications in Azure Active Directory (Azure AD), if the Azure Services onboarding dialog box immediately fails after you select **Sign in**, update the .NET Framework, and enable strong cryptography. After you make the changes, remember to restart the computers.

Configuration Manager cloud services and TLS 1.2

Starting in version 1802, the Azure virtual machines used by the cloud management gateway and cloud distribution points support TLS 1.2. Supported clients on version 1802 or later automatically use TLS 1.2.

The **SMSAdminui.log** may contain an error similar to the following example:

```
Microsoft.ConfigurationManager.CloudBase.AAD.AADAuthenticationException
Service returned error. Check InnerException for more details
at Microsoft.ConfigurationManager.CloudBase.AAD.AADAuthenticationContext.GetAADAuthResultObject
...
Microsoft.IdentityModel.Clients.ActiveDirectory.AdalServiceException
Service returned error. Check InnerException for more details
at Microsoft.IdentityModel.Clients.ActiveDirectory.AuthenticationContext.RunAsyncTask
...
System.Net.WebException
The underlying connection was closed: An unexpected error occurred on a receive.
at System.Net.HttpWebRequest.GetResponse
```

In the System EventLog, SChannel EventID 36874 may be logged with the following description:

```
An TLS 1.2 connection request was received from a remote client application, but none of the cipher suites
supported by the client application are supported by the server. The TLS connection request has failed.
```

See also

- Transport layer security (TLS) best practices with the .NET Framework
- KB 3135244: TLS 1.2 support for Microsoft SQL Server
- Cryptographic controls technical reference

Evaluate System Center Configuration Manager by building your own lab environment

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Learn how to create a lab environment to evaluate System Center Configuration Manager for use in your organization.

System Center Configuration Manager is a complex and powerful tool to manage your users, devices, and software. It's a good idea to thoroughly evaluate System Center Configuration Manager before full deployment, so that you can marry conceptual understanding with hands-on exercises.

This guide is primarily meant for admins who are evaluating the use of Configuration Manager in corporate environments:

- Admins who want a solution to fully manage PCs, servers, and mobile devices
- Admins in high-security industries that require the security of on-premises device management with the flexibility of cloud-based device management
- Admins who want to manage the scaling-up of their on-premises server architecture

What this lab does

The main goal of creating this lab environment is to give you the general knowledge to start working with Configuration Manager, and to enhance your understanding of Configuration Manager. You'll walk through an expedited assembly of the current version of Configuration Manager, by using two servers:

- One that hosts Active Directory, the domain controller, and the DNS server
- One that hosts Configuration Manager and all associated SQL Server components

Client machines are installed within Hyper-V. The lab itself can also be run as a fully virtualized system on a single server.

What this lab does not do

This lab will not take you through all Configuration Manager scenarios. It is not designed to be immediately migrated into an active environment.

When you build this lab, you will have a functional environment to work in. But this environment will not be optimized for factors like system performance, hard disk space management, and SQL Server storage.

Recommended reading before you build the lab

There is a wealth of content available in Documentation for System Center Configuration Manager. We recommend that you read the following topics from this library before you start to build the lab:

- Learn core concepts about the Configuration Manager console, end-user portals, and example scenarios in Introduction to System Center Configuration Manager.
- Learn about the primary management capabilities of Configuration Manager in Features and capabilities of

System Center Configuration Manager.

- Bolster your knowledge with Fundamentals of System Center Configuration Manager.
- Learn the importance of security roles in Fundamentals of role-based administration for System Center Configuration Manager.
- Learn about content management in Concepts for content management.
- Learn how to successfully support daily tasks throughout your deployment in Understand how clients find site resources and services for System Center Configuration Manager.

Set up your System Center Configuration Manager lab

9/5/2019 • 12 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Following the guidance in this topic will enable you to set up a lab for evaluating Configuration Manager with simulated real-life activities.

Core components

Setting up your environment for System Center Configuration Manager requires some core components to support the installation of Configuration Manager.

- **The lab environment uses Windows Server 2012 R2**, into which we will install System Center Configuration Manager.

  You can download an evaluation version of Windows Server 2012 R2 from the TechNet Evaluation Center.

  Consider modifying or disabling Internet Explorer Enhanced Security Configuration in order to more easily access some of the downloads referenced throughout the course of these exercises. Please review Internet Explorer: Enhanced Security Configuration for additional information.

- **The lab environment uses SQL Server 2012 SP2** for the site database.

  You can download an evaluation version of SQL Server 2012 from the Microsoft Download Center.

  SQL Server has Supported versions of SQL Server that must be met for use with System Center Configuration Manager.

  - Configuration Manager requires a 64-bit version of SQL Server to host the site database.
  - **SQL_Latin1_General_CP1_CI_AS** as the **SQL Collation** class.
  - **Windows authentication**, rather than SQL authentication, is required.
  - A dedicated **SQL Server instance** is required.
  - Do not limit the **system addressable memory** for SQL Server.
  - Configure the **SQL Server service account** to run using a low rights domain user account.
  - You must install **SQL Server reporting services**.
  - **Intersite communications** use the SQL Server Service Broker on default port TCP 4022.
  - **Intrasite communications** between the SQL Server database engine and select Configuration Manager site system roles use default port TCP 1433.

- **The domain controller uses Windows Server 2008 R2** with Active Directory Domain Services installed. The domain controller also functions as the host for the DHCP and the DNS servers for use with a fully qualified domain name.

  For additional information, review this overview of Active Directory Domain Services.

- **Hyper-V is used with a few virtual machines** to verify that the management steps taken in these

exercises are functioning as expected. A minimum of three virtual machines is recommended, with Windows 7 (or later) installed.

For additional information, review this overview of Hyper-V.

- **Administrator permissions** will be required for all of these components.
  - Configuration Manager requires an administrator with local permissions within the Windows Server environment
  - Active Directory requires an administrator with permissions to modify the schema
  - Virtual machines require local permissions on the machines themselves

Though not required for this lab, you can review Supported configurations for System Center Configuration Manager for additional information on requirements for implementing System Center Configuration Manager. Refer to documentation for software versions other than those referenced here.

Once you have installed all of these components, there are additional steps you must take to configure your Windows environment for Configuration Manager:

Prepare Active Directory content for the lab

For this lab, you will create a security group, then add a domain user to it.

- Security group: **Evaluation**
  - Group scope: **Universal**
  - Group type: **Security**
- Domain user: **ConfigUser**

  Under normal circumstances, you would not grant universal access to all users within your environment. You are doing so with this user in order to streamline bringing your lab online.

The next steps required to enable Configuration Manager clients to query Active Directory Domain Services to locate site resources are listed over the next procedures.

Create the System Management container

Configuration Manager will not automatically create the required System Management container in Active Directory Domain Services when the schema is extended. Therefore, you will create this for your lab. This step will require you to install ADSI Edit.

Ensure that you are logged on as an account that has **Create All Child Objects** permission on the **System** Container in Active Directory Domain Services.

To create the System Management container:

1. Run **ADSI Edit**, and connect to the domain in which the site server resides.
2. Expand **Domain<computer fully qualified domain name>**, expand **<distinguished name>**, right-click **CN=System**, click **New**, and then click **Object**.
3. In the **Create Object** dialog box, select **Container**, and then click **Next**.
4. In the **Value** box, type **System Management**, and then click **Next**.
5. Click **Finish** to complete the procedure.

Set security permissions for the System Management container

Grant the site server's computer account the permissions that are required to publish site information to the container. You will use ADSI Edit for this task as well.

> **IMPORTANT**
> Confirm that you are connected to the site server's domain prior to beginning the following procedure.

To set security permissions for the System Management container:

1. In the console pane, expand the **site server's domain**, expand **DC=<server distinguished name>**, and then expand **CN=System**. Right-click **CN=System Management**, and then click **Properties**.
2. In the **CN=System Management Properties** dialog box, click the **Security** tab, and then click **Add** to add the site server computer account. Grant the account **Full Control** permissions.
3. Click **Advanced**, select the site server's computer account, and then click **Edit**.
4. In the **Apply onto** list, select **This object and all descendant objects**.
5. Click **OK** to close the **ADSI Edit** console and complete the procedure.

   For additional insight into this procedure, please review Extend the Active Directory schema for System Center Configuration Manager

Extend the Active Directory schema using extadsch.exe

You will extend the Active Directory schema for this lab, as this allows you to use all Configuration Manager features and functionality with the least amount of administrative overhead. Extending the Active Directory schema is a forest-wide configuration that is done one time per forest. Extending the schema permanently modifies the set of classes and attributes in your base Active Directory configuration. This action is irreversible. Extending the schema allows Configuration Manager to access components that will allow it to function most effectively within your lab environment.

> **IMPORTANT**
> Ensure that you are logged on to the schema master domain controller with an account that is a member of the **Schema Admins** security group. Attempting to use alternate credentials will fail.

To extend the Active Directory schema using extadsch.exe:

1. Create a backup of the schema master domain controller's system state. For more information about backing up master domain controller, please review Windows Server Backup
2. Navigate to **\SMSSETUP\BIN\X64** in the installation media.
3. Run **extadsch.exe**.
4. Verify that the schema extension was successful by reviewing the **extadsch.log** located in the root folder of the system drive.

   For additional insight into this procedure, please review Extend the Active Directory schema for System Center Configuration Manager.

Other required tasks

You will also need to complete the following tasks prior to installation.

Create a folder for storing all downloads

There will be multiple downloads required for components of the installation media throughout this exercise. Before beginning any installation procedures, determine a location that will not require you to move these files until you wish to decommission your lab. A single folder with separate subfolders to store these downloads is recommended.

Install .NET and activate Windows Communication Foundation

You will need to install two .NET Frameworks: first, .NET 3.5.1 and then .NET 4.5.2+. You will also need to activate Windows Communication Foundation (WCF). WCF is designed to offer a manageable approach to distributed computing, broad interoperability, and direct support for service orientation, and simplifies development of connected applications through a service-oriented programming model. Please review What Is Windows Communication Foundation? for additional insight into WCF.

To install .NET and activate Windows Communication Foundation:

1. Open **Server Manager**, then navigate to **Manage**. Click **Add Roles and Features** to open the **Add Roles and Features Wizard.**
2. Review the information provided in the **Before You Begin** panel, then click **Next**.
3. Select **Role-based or feature-based installation**, then click **Next**.
4. Select your server from the **Server Pool**, then click **Next**.
5. Review the **Server Roles** panel, then click **Next**.
6. Add the following **Features** by selecting them from the list:
    - **.NET Framework 3.5 Features**
        - **.NET Framework 3.5 (includes .NET 2.0 and 3.0)**
    - **.NET Framework 4.5 Features**
        - **.NET Framework 4.5**
        - **ASP.NET 4.5**
        - **WCF Services**
            - **HTTP Activation**
            - **TCP Port Sharing**
7. Review the **Web Server Role (IIS)** and **Role Services** screen, then click **Next**.
8. Review the **Confirmation** screen, then click **Next**.
9. Click **Install** and verify that the installation completed properly in the **Notifications** pane of **Server Manager**.
10. After the base installation of .NET completes, navigate to the Microsoft Download Center to obtain the web installer for the .NET Framework 4.5.2. Click the **Download** button, then **Run** the installer. It will automatically detect and install the required components in your selected language.

For additional information, please review the following articles for why these .NET Frameworks are required:

- .NET Framework Versions and Dependencies
- .NET Framework 4 RTM Application Compatibility Walkthrough
- How to: Upgrade an ASP.NET Web Application to ASP.NET 4

- Microsoft .NET Framework Support Lifecycle Policy FAQ
- CLR Inside Out - In-Process Side-by-Side

Enable BITS, IIS, and RDC

The Background Intelligent Transfer Service (BITS) is used for applications that need to transfer files asynchronously between a client and a server. By metering the flow of the transfers in the foreground and background, BITS preserves the responsiveness of other network applications. It will also automatically resume file transfers if a transfer session is interrupted.

You will install BITS for this lab, as this site server will also be used as a management point.

Internet Information Services (IIS) is a flexible, scalable web server that can be used to host anything on the web. It is used by Configuration Manager for a number of site system roles. For additional information on IIS, review Websites for site system servers in System Center Configuration Manager.

Remote Differential Compression (RDC) is a set of APIs that applications can use to determine if any changes have been made to a set of files. RDC enables the application to replicate only the changed portions of a file, keeping network traffic to a minimum.

To enable BITS, IIS, and RDC site server roles:

1. On your site server, open **Server Manager**. Navigate to **Manage**. Click **Add Roles and Features** to open the **Add Roles and Features Wizard**.
2. Review the information provided in the **Before You Begin** panel, then click **Next**.
3. Select **Role-based or feature-based installation**, then click **Next**.
4. Select your server from the **Server Pool**, then click **Next**.
5. Add the following **Server Roles** by selecting them from the list:
    - **Web Server (IIS)**
        - **Common HTTP Features**
            - **Default Document**
            - **Directory Browsing**
            - **HTTP Errors**
            - **Static Content**
            - **HTTP Redirection**
        - **Health and Diagnostics**
            - **HTTP Logging**
            - **Logging Tools**
            - **Request Monitor**
            - **Tracing**
    - **Performance**
        - **Static Content Compression**
        - **Dynamic Content Compression**
    - **Security**

    - **Request Filtering**
    - **Basic Authentication**
    - **Client Certificate Mapping Authentication**
    - **IP and Domain Restrictions**
    - **URL Authorization**
    - **Windows Authentication**
- **Application Development**
    - **.NET Extensibility 3.5**
    - **.NET Extensibility 4.5**
    - **ASP**
    - **ASP.NET 3.5**
    - **ASP.NET 4.5**
    - **ISAPI Extensions**
    - **ISAPI Filters**
    - **Server Side Includes**
- **FTP Server**
    - **FTP Service**
- **Management Tools**
    - **IIS Management Console**
    - **IIS 6 Management Compatibility**
        - **IIS 6 Metabase Compatibility**
        - **IIS 6 Management Console**
        - **IIS 6 Scripting Tools**
        - **IIS 6 WMI Compatibility**
    - **IIS 6 Management Scripts and Tools**
    - **Management Service**

6. Add the following **Features** by selecting them from the list:
    - **Background Intelligent Transfer Service (BITS)**
        - **IIS Server Extension**
    - **Remote Server Administration Tools**
        - **Feature Administration Tools**
        - **BITS Server Extensions Tools**
7. Click **Install** and verify that the installation completed properly in the **Notifications** pane of **Server Manager**.

By default, IIS blocks several types of file extensions and locations from access by HTTP or HTTPS communication. To enable these files to be distributed to client systems, you will need to configure request filtering for IIS on your distribution point. For more information, please review IIS Request Filtering for distribution points.

To configure IIS filtering on distribution points:

1. Open **IIS Manager** and select the name of your server in the sidebar. This will take you to the **Home** screen.
2. Verify that **Features View** is selected at the bottom of the **Home** screen. Navigate to **IIS** and open **Request Filtering**.
3. In the **Actions** pane, click **Allow File Name Extension...**
4. Type **.msi** into the dialog box and click **OK**.

Installing Configuration Manager

You will create a Determine when to use a primary site to manage clients directly. This will allow your lab environment to support management for Site system scale of potential devices.
During this process, you will also install the Configuration Manager console, which will be used to manage your evaluation devices going forward.

Before you begin the installation, launch the Prerequisite Checker on the server using Windows Server 2012 to confirm that all settings have been correctly enabled.

To download and install Configuration Manager:

1. Navigate to the System Center Evaluations page to download the newest evaluation version of System Center Configuration Manager.
2. Decompress the download media into your predefined location.
3. Follow the installation procedure listed at Install a site using the System Center Configuration Manager Setup Wizard. Within that procedure, you will input the following:

STEP IN SITE INSTALLATION PROCEDURE	SELECTION
Step 4: the **Product Key** page	Select **Evaluation**.
Step 7: **Prerequisite Downloads**	Select **Download required files** and specify your predefined location.
Step 10: **Site and Installation Settings**	- **Site code:LAB** - **Site name:Evaluation** - **Installation folder:** specify your predefined location.
Step 11: **Primary Site Installation**	Select **Install the primary site as a stand-alone site**, then click **Next**.
Step 12: **Database Installation**	- **SQL Server name (FQDN):** input your FQDN here. - **Instance name:** leave this blank, as you will use the default instance of SQL that you previously installed. - **Service Broker Port:** leave as default port of 4022.
Step 13: **Database Installation**	Leave these settings as default.
Step 14: **SMS Provider**	Leave these settings as default.

STEP IN SITE INSTALLATION PROCEDURE	SELECTION
Step 15: **Client Communication Settings**	Confirm that **All site system roles accept only HTTPS communication from clients** is not selected
Step 16: **Site System Roles**	Input your FQDN and confirm that your selection of **All site system roles accept only HTTPS communication from clients** is still deselected.

Enable publishing for the Configuration Manager site

Each Configuration Manager site publishes its own site-specific information to the System Management container within its domain partition in the Active Directory schema. Bidirectional channels for communication between Active Directory and Configuration Manager must be opened to handle this traffic. You will also additionally enable Forest Discovery to determine certain components of your Active Directory and network infrastructure.

To configure Active Directory forests for publishing:

1. In the bottom-left corner of the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Hierarchy Configuration**, then click **Discovery Methods**.
3. Select **Active Directory Forest Discovery** and click **Properties**.
4. In the **Properties** dialog box, select **Enable Active Directory Forest Discovery**. Once this is active, select **Automatically create Active Directory site boundaries when they are discovered**. A dialog box will appear that states **Do you want to run full discovery as soon as possible?** Click **Yes**.
5. In the **Discovery Method** group at the top of the screen, click **Run Forest Discovery Now**, then navigate to **Active Directory Forests** in the sidebar. Your Active Directory forest should be shown in the list of discovered forests.
6. Navigate to the top of the screen, to the **General** tab.
7. In the **Administration** workspace, expand **Hierarchy Configuration**, then click **Active Directory Forests**.

To enable a Configuration Manager site to publish site information to your Active Directory forest:

1. In the Configuration Manager console, click **Administration**.
2. You will configure a new forest that has not yet been discovered.
3. In the **Administration** workspace, click **Active Directory Forests**.
4. On the **Publishing** tab of the site properties, select your connected forest, then click **Ok** to save the configuration.

Create a Configuration Manager lab in Azure

7/23/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Technical Preview)

This guide describes how to build a Configuration Manager lab environment in Microsoft Azure. It uses Azure templates to simplify and automate the creation of a lab using Azure resources. Two Azure templates are provided:

- Configuration Manager technical preview Azure template installs the latest version of the Configuration Manager technical preview branch.
- Configuration Manager current branch Azure template installs the evaluation of the latest version of Configuration Manager current branch.

For more information, see Configuration Manager on Azure.

Prerequisites

This process requires an Azure subscription in which you can create the following objects:

- Two Standard_B2s virtual machines for Domain Contoller and MP & DP roles.
- One Standard_B2ms virtual machine for Primary Site Server and SQL database server.
- Standard_LRS storage account

> **TIP**
> See the Azure pricing calculator to help determine potential costs.

Process

1. Go to the Configuration Manager technical preview template or Configuration Manager current branch template.
2. Select **Deploy to Azure**, which opens the Azure portal.
3. Complete the Azure quickstart template with the following information:
   - Basics
     - **Subscription**: The name of the subscription in which to create the VMs
     - **Resource group**: Select a resource group to use for these VMs
     - **Location**: Select an Azure data center to host this lab environment
   - Settings
     - **Prefix**: The prefix name of the machines. For more information, see Azure VM info.
     - **Admin Username**: The name of a user on the VMs with administrative rights. You use this user to sign in to the VMs.
     - **Admin Password**: The password must meet the Azure complexity requirements. For more information, see adminPassword.

> **IMPORTANT**
>
> The following settings are required by Azure. Use the default values. Don't change these values.
>
> - **_artifacts Location**: The location of the scripts for this template
> - **_artifacts Location Sas Token**: The sasToken is required to access the artifacts location
> - **Location**: The location for all resources

4. Read the terms and conditions. If you agree, select **I agree to the terms and conditions stated above**. Then select **Purchase** to continue.

Azure validates the settings, and then begins the deployment. Check the status of the deployment in the Azure portal. The process can take 2-4 hours. Even when the Azure portal shows successful deployment, configuration scripts continue to run. Don't restart the VMs during the process.

To see the status of the configuration scripts, connect to the `<prefix>PS1` server, and view the following file: `%windir%\TEMP\ProvisionScript\PS1.json`. If it shows all steps as complete, the process is done.

To connect to the VMs, first get from the Azure portal the public IP addresses for each VM. When you connect to the VM, the domain name is `contoso.com`. Use the credentials that you specified in the deployment template. For more information, see How to connect and log on to an Azure virtual machine running Windows.

Azure VM info

All Three VMs have the following specifications:

- 150 GB of disk space
- Both a public and private IP address. The public IPs are in a network security group that only allows remote desktop connections on TCP port 3389.

The prefix that you specified in the deployment template is the VM name prefix. For example, if you set "contoso" as the prefix, then the domain controller machine name is `contosoDC`.

`<prefix>DC01`

- Active Directory domain controller
- Standard_B2s, which has two CPU and 4 GB of memory
- Windows Server 2019 Datacenter edition

Windows features and roles

- Active Directory Domain Services (ADDS)
- .NET
- Remote Differential Compression (RDC)

`<prefix>PS01`

- Standard_B2ms, which has two CPU and 8 GB of memory
- Windows Server 2016 Datacenter edition
- SQL Server
- Windows 10 ADK with Windows PE
- Configuration Manager primary site

Windows features and roles

- .NET
- Remote Differential Compression (RDC)

- Internet Information Service (IIS)

`<prefix>DPMP01`

- Standard_B2s, which has two CPU and 4 GB of memory
- Windows Server 2019 Datacenter edition
- Distribution point
- Management point

Windows features and roles

- .NET
- Remote Differential Compression (RDC)
- Internet Information Service (IIS)
- Background intelligent transfer service (BITS)

`<prefix>CL01`

- Only for Configuration Manager current branch evaluation template
- Windows 10
- Configuration Manager client

Technical preview for Configuration Manager

8/30/2019 • 7 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Technical Preview)

This article provides details about the monthly technical preview branch of Configuration Manager. The technical preview introduces new functionality that Microsoft is working on. It introduces new features that aren't yet included in the current branch of Configuration Manager. These features might eventually be included in an update to the current branch. Before we finalize the features, we want you to try them out and give us feedback.

Because this release is a technical preview, details and functionality are subject to change.

This information applies to all versions of the Configuration Manager technical preview branch. This article lists each new feature along with the technical preview version in which it first appears. For example, version **1908** for August (08) of 2019 (19). Separate articles dedicated to each preview version detail the individual features.

For information about what's new in the *current branch* of Configuration Manager, see What's new in Configuration Manager incremental versions.

TIP

To get notified when this page is updated, copy and paste the following URL into your RSS feed reader:

```
https://docs.microsoft.com/api/search/rss?search=%22technical+preview+releases+-
+Configuration+Manager%22&locale=en-us
```

Requirements and limitations

IMPORTANT

The technical preview is licensed for use only in a lab environment. Microsoft may not provide support services and certain features may not be available in technical previews. Additionally, technical preview software may have reduced or different security, privacy, accessibility, availability, and reliability standards relative to commercially provided software.

For most product prerequisites, use the information in the Supported configurations. The following exceptions apply to the technical preview branch:

- Each install is active for 90 days before it becomes inactive.
- English is the only language supported.
- It only supports the following setup command-line parameters:
  - `/silent`
  - `/testdbupgrade`
- The service connection point installs to online mode. It doesn't support offline mode.
- The separate articles for each specific version of the technical preview include additional limitations or requirements, as applicable.
- The following features aren't supported with the technical preview branch:
  - Migration to or from this preview branch.

    - Upgrade to this preview branch.
    - Site recovery from the cd.latest folder.
- There's no support for updating to current branch from this preview branch.

> **NOTE**
> When updates are available for a preview version, you still find and install them from the **Updates and Servicing** node of the Configuration Manager console. For a video of the in-console upgrade process, see Installing Configuration Manager update packages on youtube.com.

- It only supports a standalone primary site. There's no support for a central administration site, multiple primary sites, or secondary sites.

The technical preview branch of Configuration Manager supports the following products and technologies:

- It only supports the following versions of **SQL Server**:
    - SQL Server 2017 (with cumulative update 2 or later)
    - SQL Server 2016 (with no service pack or later)
    - SQL Server 2014 (with service pack 1 or later)
    - SQL Server 2012 (with service pack 3 or later)
- The site supports up to 10 clients, which must run one of the following versions of Windows:
    - Windows 10
    - Windows 8.1
    - Windows 7

> **NOTE**
> The inclusion of these products in this content doesn't imply an extension of support for a version that's beyond its support lifecycle. Configuration Manager doesn't support products that are beyond their support lifecycle. For more information, see Microsoft Lifecycle Policy.

Install and update

The Configuration Manager technical preview branch for lab use is distinct from the Configuration Manager current branch for production use.

First install a baseline version of the technical preview branch. After installing a baseline version, then use in-console updates to bring your installation up-to-date with the most recent preview version. Typically, new versions of the technical preview are available each month.

Microsoft supports each technical preview version up until three successive versions are available. For example, when version 1708 released, version 1704 was no longer in support. Versions 1705, 1706, and 1707 remained in support. When a baseline falls out of support, it's still supported for installing a new technical preview site, assuming you immediately update to a supported version. The older baseline is supported until a new baseline version is available. Update to the latest available version from the baseline, and then repeat the update process until you install the latest technical preview version.

> **TIP**
> When you install an update to the technical preview, you update your preview installation to that new technical preview version. A technical preview installation never has the option to upgrade to a current branch installation. It also never receives updates from the current branch release.
>
> Several times throughout the year, there are technical preview branch and current branch versions with the same version number. For example, there is a technical preview version 1802 and a current branch version 1802.

Active baseline versions

Install a baseline version for up to one year after its release. When you install a new technical preview site, if more than one baseline version is currently available, use the latest baseline version.

- **Technical preview version 1907**: The Configuration Manager technical preview version 1907 is available as both an in-console update and as a new baseline version. Download baseline versions from the TechNet Evaluation Center.

Providing feedback

We love to hear your feedback about the new features in the technical preview. For more information, see Product feedback.

If you have ideas about new features you would like to see, we want to know that as well. To submit new ideas and to vote on the ideas submitted by others, visit our UserVoice page.

Features in the most recent version

The following features are available with the most recent Configuration Manager technical preview version:

Technical preview version 1908.2

- Improvements to Console Connections
- Improvements to multicast-enabled distribution points
- Optimizations to the CMPivot engine
- Set keyboard layout during OS deployment

> **NOTE**
> Features that were available in a previous version of the technical preview remain available in later versions. Similarly, features that are added to the Configuration Manager current branch remain available in the technical preview branch.

Features in recent technical previews

The following features were released with previous versions of the Configuration Manager technical preview branch since current branch version 1906:

Technical preview version 1908

- Task sequence performance improvements for power plans
- Local device query evaluation using CMPivot standalone
- Additional software update filter for ADRs
- Use Delivery Optimization for all Windows updates
- Phased deployment templates
- Improvements to console connections node

- Copy and paste task sequence conditions
- Improvements to task sequence search
- Improvements to OS deployment

Technical preview version 1907

- Search the task sequence editor
- Improvements to Office 365 ProPlus upgrade readiness dashboard

> **TIP**
> When a new current branch version is available, features that are available in that version are listed in the latest *What's new* article. For more information, see What's new in incremental versions.

Features in previous technical previews

The following features were released with previous versions of the Configuration Manager technical preview branch. These features remain available in later versions, but aren't yet available in the current branch.

FEATURE	TECHNICAL PREVIEW VERSION
Remote control anywhere using cloud management gateway	Tech Preview 1906
Improvements to Community Hub	Tech Preview 1906
Additional options for third-party update catalogs	Tech Preview 1906
Task sequence as an app model deployment type	Tech Preview 1905
BitLocker management	Tech Preview 1905
Improvements to Community Hub	Tech Preview 1905
Community Hub and GitHub	Tech Preview 1904
Cloud services cost estimator	Tech Preview 1903
Download reports from the Community Hub	Tech Preview 1812
Community Hub	Tech Preview 1807
Client-based PXE responder service	Tech Preview 1712
PXE network boot support for IPv6	Tech Preview 1706
Use Azure Active Directory	Tech Preview 1702
Improvements to Asset Intelligence	Tech Preview 1608

See also

For more information, see the following articles:

- Evaluate Configuration Manager in a lab
- What's new in Configuration Manager incremental versions
- Introduction to Configuration Manager

> **TIP**
>
> For more information on current branch features that require consent to enable, see pre-release features.
>
> For more information on current branch features that you must enable first, see Enable optional features from updates.

Features in Configuration Manager technical preview version 1908.2

8/30/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Technical Preview)

This article introduces the features that are available in the technical preview for Configuration Manager, version 1908.2. Install this version to update and add new features to your technical preview site.

Review the technical preview article before installing this update. That article familiarizes you with the general requirements and limitations for using a technical preview, how to update between versions, and how to provide feedback.

The following sections describe the new features to try out in this version:

Improvements to Console Connections

We've made the following improvements to **Console Connections**:

- The ability to message other administrators through Microsoft Teams.
- The **Last Console Heartbeat** column has replaced the **Last Connected Time** column.
  - An open console in the foreground sends a heartbeat every 10 minutes.

Prerequisites

- The Administration Service must be enabled for the **Last Console Heartbeat** to function.
- For messaging administrators, the account you want to message needs to have been discovered with Azure AD or AD User Discovery.

Log files

For troubleshooting, refer to the **SmsAdminUI.log**.

Known issues

The error message notifying you that Microsoft Teams isn't installed won't be displayed if the following Registry key doesn't exist:

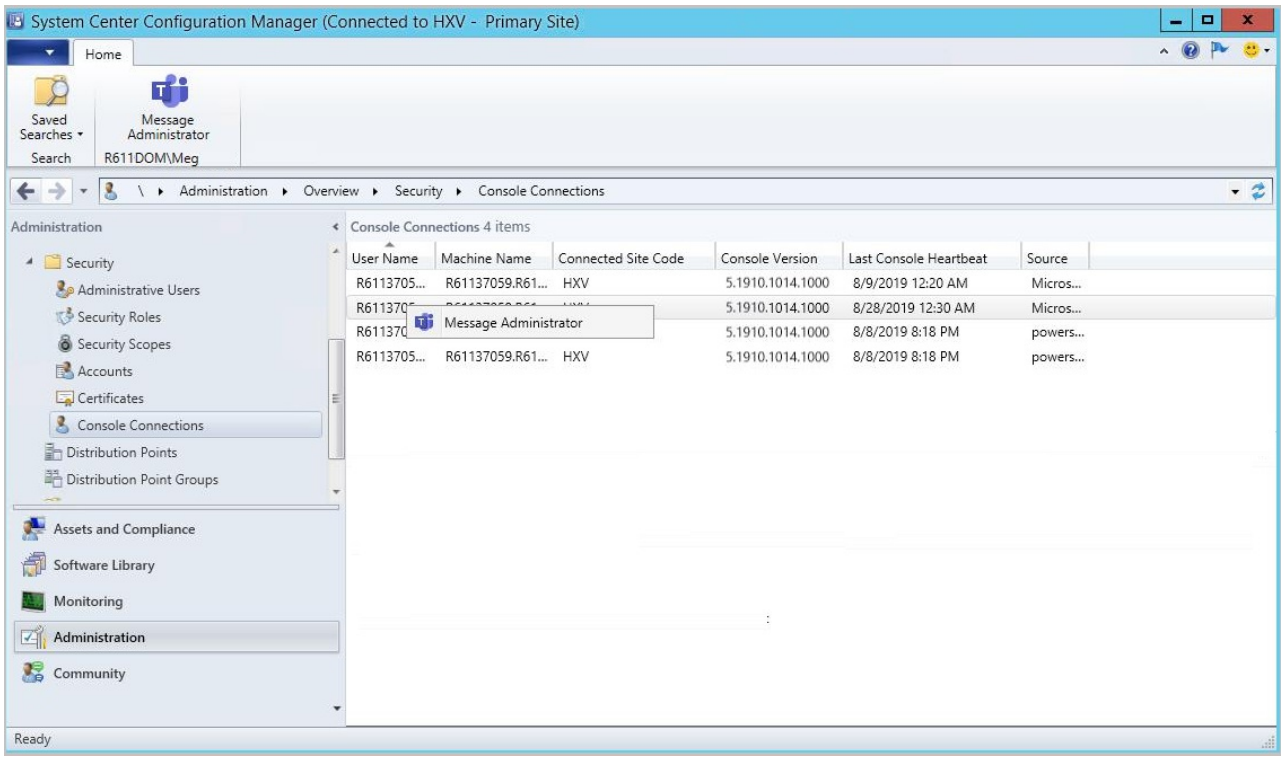
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

To work around the issue, manually create the Registry key.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. Go to **Administration** > **Security** > **Console Connections**.
2. Notice the column **Last Console Heartbeat** has replaced the **Last Connected Time** column.
3. Right-click on a user's console connection and select **Message Administrator**.
   - If the User Principal Name isn't found for the selected administrator, **Message Administrator** is grayed out.
   - An error message, including a download link, appears if Microsoft Teams isn't installed on the device from which you run the console.
   - If Microsoft Teams is installed on the device from which you run the console, it will open a chat with the user.



Improvements to multicast-enabled distribution points

You can now enable multicast on a distribution point without installing Windows Deployment Services (WDS). Because WDS isn't required, the multicast-enabled distribution point can be a client or server OS, including Windows Server Core. It can also receive multicast content in the full OS, it's not limited to only Windows PE.

Prerequisites

The distribution point and Configuration Manager client use the following network ports:

- TCP 27500-27755
- UDP 27500-27755
- UDP 64001-64256

Make sure your network infrastructure allows the use of these ports.

> **NOTE**
> You don't have to enable the PXE responder. In this release, when you enable multicast, it always uses this new multicast server.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

Enable multicast on the distribution point

1. In the Configuration Manager console, go to the **Administration** workspace, and select the **Distribution Points** node. Select the target distribution point, and select **Properties** in the ribbon.
2. Switch to the **Multicast** tab, and select the option to **Enable multicast to simultaneously send data to multiple clients**.
3. Select **OK** to save the settings.

For more information about the additional multicast settings, see Install and configure distribution points.

Enable packages to use multicast

The following content types support multicast:

- Packages
- Driver packages
- OS images
- OS upgrade packages

Enable any package that you want to distribute via multicast:

1. Open the **Properties** of the target package and switch to the **Distribution Settings** tab.
2. In the OS deployment settings section, enable the option to **Allow this package to be transferred via multicast**.

Distribute these multicast-enabled packages to a multicast-enabled distribution point.

Deploy a task sequence

Configure a task sequence deployment that references these multicast-enabled packages. On the **Distribution Points** tab of the deployment properties, select the deployment option to **Download content locally when needed by the running task sequence**.

For more information, see Deploy a task sequence.

Monitor the multicast deployment

On the distribution point, there's a new log file, **McsServer.log**. This file includes details of multicast download sessions.

On the client, review the **smsts.log** file for entries from the **McsClient** component.

Known issues

After you configure multicast on a distribution point, confirm the following settings in the registry key `HKLM\Software\Microsoft\SMS\DP`:

- The value `IsMulticast` should be `1`.
- The permissions on the `SccmMcs` key should have the **Local Service** account with **Full Control**.

This multicast provider doesn't support IPv6. Disable the IPv6 protocol on any multicast-enabled distribution point.

Optimizations to the CMPivot engine

We've added some significant optimizations to the CMPivot engine that allows us to push more of the processing to the ConfigMgr client. The optimizations drastically reduce the network and server CPU load needed to run CMPivot queries. With these optimizations, we can now sift through gigabytes of client data in real time.

Examples

You can search all event logs on all clients in your enterprise for authentication failures with the following query:

```
EventLog('Security')
| where  EventID == 4673
| summarize count() by Device
| order by count_ desc
```

Search for a file by hash:

```
Device
| join kind=leftouter ( File('%windir%\\system32\\*.exe')
| where Hash == 'A92056D772260B39A876D01552496B2F8B4610A0B1E084952FE1176784E2CE77')
| project Device, MalwareFound = iif( isnull(FileName), 'No', 'Yes')
```

Set keyboard layout during OS deployment

Based on your UserVoice feedback, you can now set the default keyboard layout during an OS deployment task sequence. The **Apply Windows Settings** task sequence step includes the setting to **Set default keyboard layout in Windows**.

Next steps

For more information about installing or updating the technical preview branch, see Technical preview.

For more information about the different branches of Configuration Manager, see Which branch of Configuration Manager should I use?

Features in Configuration Manager technical preview version 1908

8/6/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Technical Preview)

This article introduces the features that are available in the technical preview for Configuration Manager, version 1908. Install this version to update and add new features to your technical preview site.

Review the technical preview article before installing this update. That article familiarizes you with the general requirements and limitations for using a technical preview, how to update between versions, and how to provide feedback.

The following sections describe the new features to try out in this version:

Task sequence performance improvements for power plans

Based on your UserVoice feedback, you can now run a task sequence with the high performance power plan. This option improves the overall speed of the task sequence. It configures Windows to use its built-in high performance power plan, which delivers maximum performance at the expense of higher power consumption.

When the task sequence starts, it records the currently enabled power plan. It then switches the active power plan to the Windows default **High Performance** plan. If the task sequence restarts the computer, it repeats this process. At the end of the task sequence, it resets the power plan to the stored value. This functionality works in both Windows and Windows PE, but has no impact on virtual machines.

> **IMPORTANT**
> To take advantage of this new Configuration Manager feature, after you update the site, update clients to the latest version. Also update boot images to include the latest client components. While new functionality appears in the Configuration Manager console when you update the site and console, the complete scenario isn't functional until the client version is also the latest.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the Configuration Manager console, go to the **Software Library** workspace. Expand **Operating Systems**, and select the **Task Sequences** node.
2. Create or choose an existing task sequence, and then select **Properties**.
3. Switch to the **Performance** tab.
4. Enable the option to **Run as high performance power plan**.

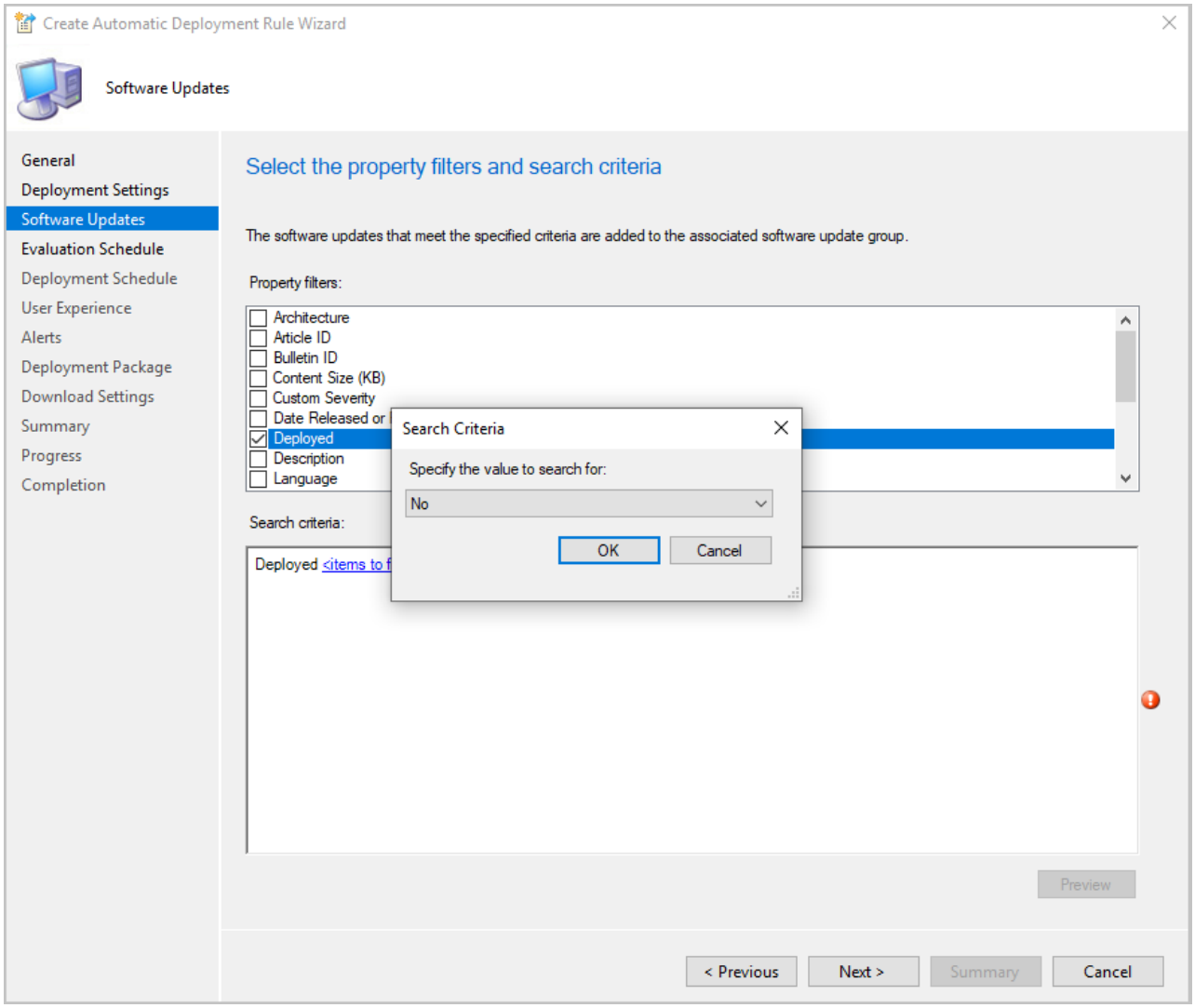
> **WARNING**
> Be cautious with this setting on low performance hardware. Running intense system operations for an extended period of time can strain low-end hardware. Check with your hardware manufacturer for specific guidance.

Local device query evaluation using CMPivot standalone

When using CMPivot outside of the Configuration Manager console, you can query just the local device without the need for the Configuration Manager infrastructure. You can now leverage the CMPivot Azure Log Analytics queries to quickly view WMI information on the local device. This also enables validation and refinement of CMPivot queries, before running them in a larger environment. CMPivot standalone is a pre-release feature and is only available in English. For more information about installing CMPivot standalone, see Install CMPivot standalone.

Additional software update filter for ADRs

As a result of your UserVoice feedback, now you can use **Deployed** as an update filter for your automatic deployment rules. This filter helps identify new updates that may need to be deployed to your pilot or test collections. The software update filter can also help avoid redeploying older updates. When using **Deployed** as a filter, be mindful that you may have already deployed the update to another collection, such as a pilot or test collection.



Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

To create a new ADR:

1. Go to **Software Library** > **Software Updates** > **Automatic Deployment Rules**.
2. In the ribbon, click **Create Automatic Deployment Rule**.
3. Specify your settings on the **General** and **Deployment Settings** pages in the wizard.
4. When you get to the **Software Updates** page, select **Deployed** and choose either **Yes** or **No**.
5. Complete the rest of your ADR selections by following the rest of the wizard.

Change an existing ADR:

1. Go to **Software Library** > **Software Updates** > **Automatic Deployment Rules**.
2. Right-click on the automatic deployment rule you want to modify and select **Properties**.
3. In the **Software Updates** tab, select **Deployed** and choose either **Yes** or **No**.
4. Click **OK** to save and close the properties page. The new filter will be used the next time the rule is run.

Use Delivery Optimization for all Windows updates

Previously, Delivery Optimization could be leveraged only for express updates. With this technical preview, it's now possible to use Delivery Optimization for the distribution of all Windows Update content for clients running Windows 10 version 1709 or later.

Prerequisites

Enable the following software updates client settings:

- **Allow clients to download delta content when available** set to **Yes**
- **Port that clients use to receive requests for delta content** set to 8005 (default) or a custom port number

Delivery Optimization must be enabled (default) and not bypassed. For more information, see Windows Delivery Optimization.

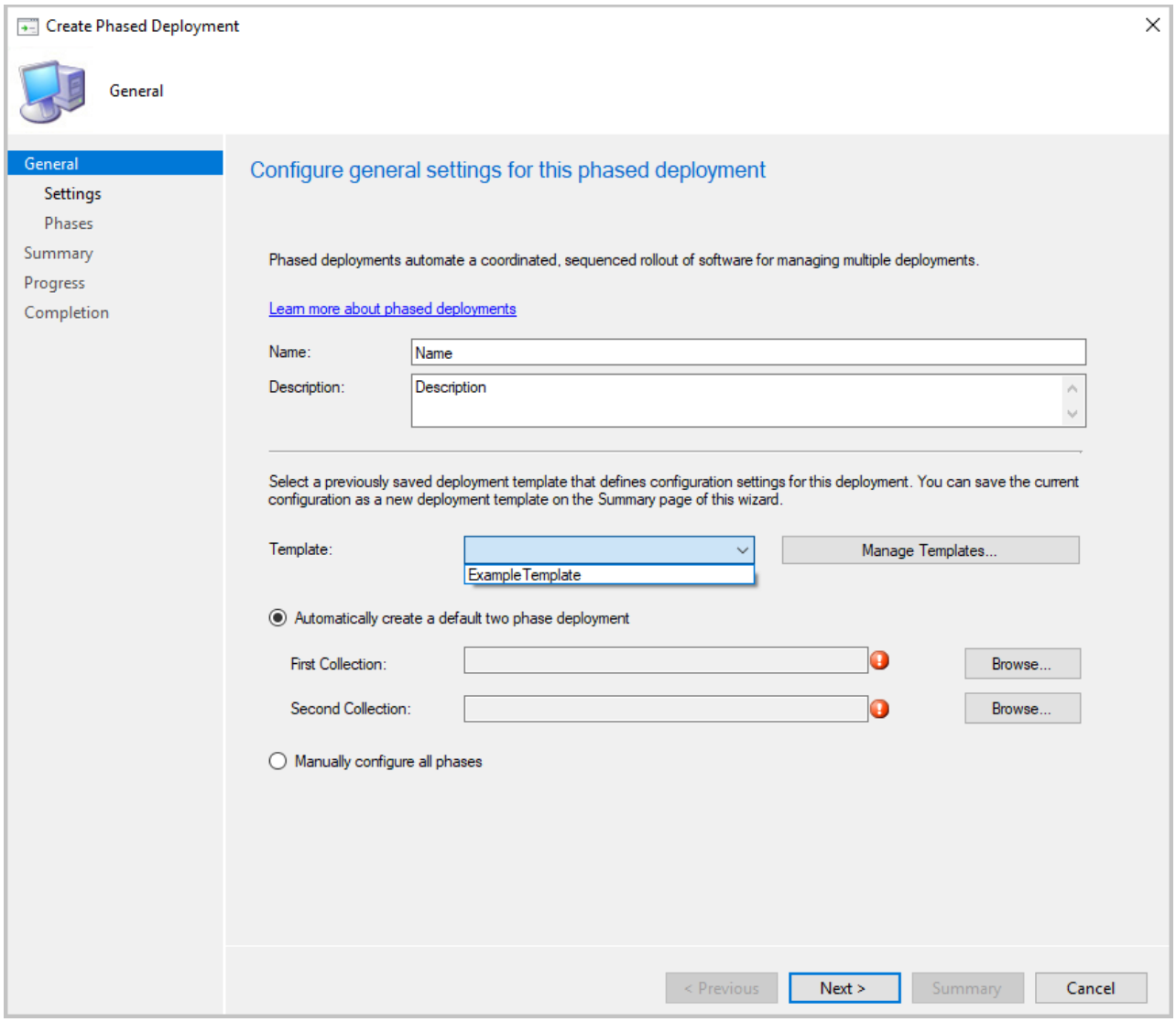
Log files

For clients running Windows 10 version 1709 or later, use the following log files to monitor delta downloads:

- WUAHandler.log
- DeltaDownload.log

Phased deployment templates

In the same way that it's possible to create deployment templates, it's now possible to create and use phased deployment templates for software updates. Templates will save you time when configuring other phased deployments with similar settings.

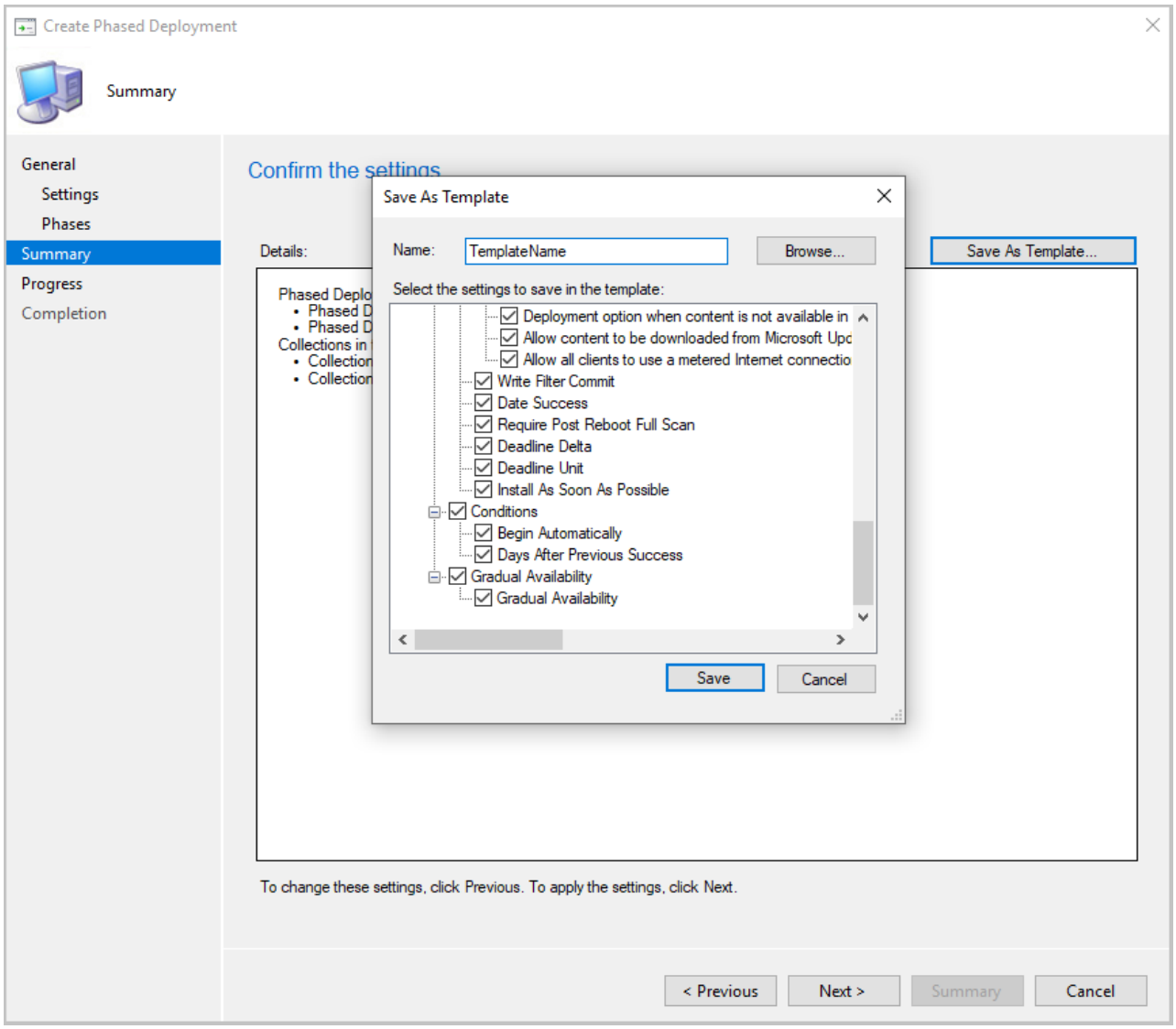


Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

Create a phased deployment template:

1. In the ribbon, select **Create Phased Deployment** for one of the following objects:
   - Task sequence
   - Software update or software update group
   - Application
2. Specify your usual settings for your phased deployment.
3. When you get to the **Summary** page, click the **Save As Template...** option.
4. Give your template a name and select which settings to save in your template.
5. Click **Save**. Use your new template the next time you create a phased deployment.



Improvements to console connections node

In the **Console Connections** node, The **Last Console Heartbeat** column has replaced **Last Connected Time**. The **Last Console Heartbeat** column gives administrators more information for determining which console connections are currently active. When a Configuration Manager console is open, a check is made every 10 minutes. If the console is running in the foreground during the check, the **Last Console Heartbeat** column is updated.

Copy and paste task sequence conditions

If you want to reuse the conditions from one task sequence step to another, based on your UserVoice feedback, you can now copy and paste conditions in the task sequence editor. Select a condition to cut or copy it. If a condition has children, it copies the entire block. If there's a condition on the clipboard, you can paste it with the following options:

- Paste before
- Paste after
- Paste under (only applies to nested conditions)

Use standard keyboard shortcuts to copy (**CTRL** + **C**) and cut (**CTRL** + **X**). The standard **CTRL** + **V** keyboard shortcut does the **Paste after** action.

There are also new options to move conditions up or down the list.

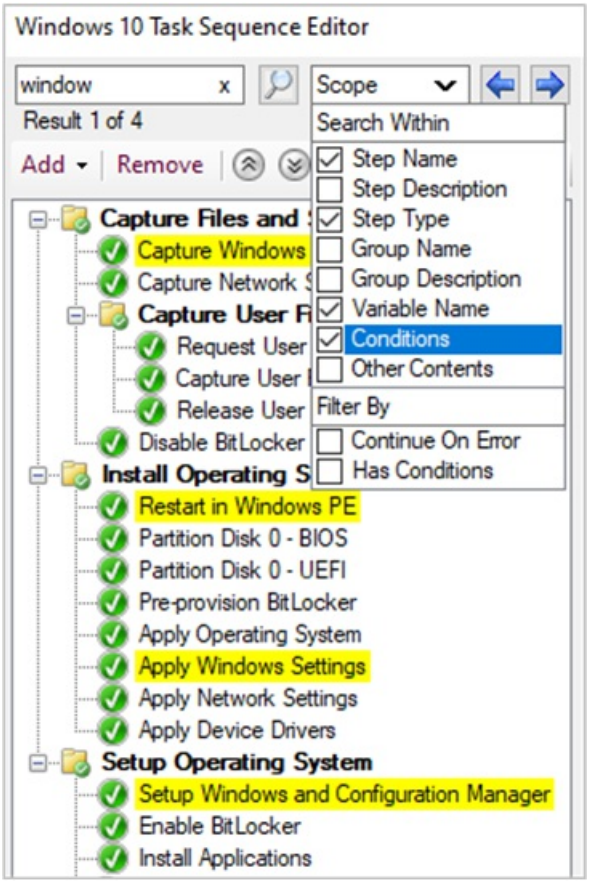
NOTE

You can copy and paste conditions between steps in a task sequence. It doesn't support this action between different task sequences.

Improvements to task sequence editor search

This release includes the following improvements to the version 1907 feature to search the task sequence editor:

- The list of search options is now named **Scope**. Use it to choose the areas of the task sequence editor to search. You can now use **Alt** + **Down arrow** to open this list.
- Instead of scoping the search to the **Group**, you can now search on **Group Name** or **Group Description**.



Improvements to OS deployment

This release includes the following improvements to OS deployment:

- Based on your UserVoice feedback, configure the default keyboard layout for a boot image. On the **Customization** tab of a boot image, use the new option to **Set default keyboard layout in WinPE**. In the console, if you select a language other than en-us, Configuration Manager still includes en-us in the available input locales. On the device, the initial keyboard layout is the selected locale, but the user can switch the device to en-us if needed.

  > **TIP**
  >
  > The Set-CMBootImage PowerShell cmdlet now includes a new parameter, `-InputLocale`. For example:
  >
  > ```
  > # Set boot image keyboard layout to Russian (Russia)
  > Set-CMBootimage -Id "CM100004" -InputLocale "ru-ru"`
  > ```

- Based on your UserVoice feedback, the **Run Command Line** step now includes an option to **Output to task sequence variable**. When you enable this option, the task sequence saves the output from the command to a custom task sequence variable that you specify.

  > **NOTE**
  >
  > Configuration Manager now limits this output to the last 1000 characters. This change applies to both the **Run Command Line** and **Run Powershell Script**. For more information, see About task sequence steps steps.

- When importing an OS upgrade package, you can **Extract a specific image index from install.wim file of selected upgrade package**. This behavior is similar as with OS images, except it overwrites the existing install.wim in the OS upgrade package. It extracts the image index to a temporary location, and then moves it into the original source directory.

  > **WARNING**
  >
  > Before you import an OS upgrade package and enable this option, make sure to backup the original source files. Configuration Manager overwrites the install.wim in the source to use the extracted image index.

- Based on your UserVoice feedback, use the following PowerShell cmdlets to automate the management of duplicate hardware identifiers:
  - New-CMDuplicateHardwareIdGuid
  - Remove-CMDuplicateHardwareIdGuid
  - New-CMDuplicateHardwareIdMacAddress
  - Remove-CMDuplicateHardwareIdMacAddress

Next steps

For more information about installing or updating the technical preview branch, see Technical preview.

For more information about the different branches of Configuration Manager, see Which branch of Configuration Manager should I use?

Features in Configuration Manager technical preview version 1907

7/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Technical Preview)

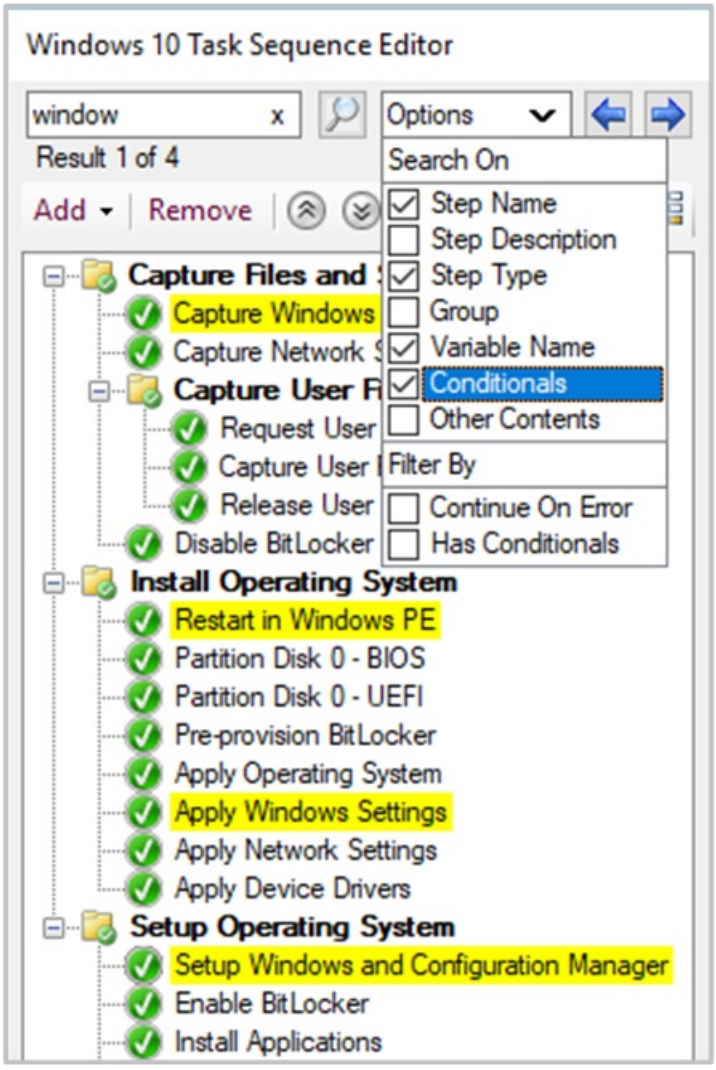
This article introduces the features that are available in the technical preview for Configuration Manager, version 1907. Install this version to update and add new features to your technical preview site.

Review the technical preview article before installing this update. That article familiarizes you with the general requirements and limitations for using a technical preview, how to update between versions, and how to provide feedback.

The following sections describe the new features to try out in this version:

Search the task sequence editor

If you have a large task sequence with many groups and steps, it can be difficult to find specific steps. Based on your UserVoice feedback, you can now search in the task sequence editor. This action lets you more quickly locate steps in the task sequence.



Search using the following criteria:

- Step name
- Step type
- Step description
- Group name
- Variable name
- Conditions
- Other content, for example, strings like variable values or command lines

You can also filter for all steps with the following attributes:

- Continue on error
- Has conditions

When you search, the editor window highlights in yellow the steps that match your search criteria.

You can quickly access these search fields and navigate the search results with the following keyboard shortcuts:

- **CTRL** + **F**: enter a search string
- **CTRL** + **O**: select the search options to scope the results
- **F3** or **Enter**: step forward through the results
- **SHIFT** + **F3**: step backwards through the results

Improvements to Office 365 ProPlus upgrade readiness dashboard

We've made improvements to the **Office 365 ProPlus upgrade readiness** dashboard that released in Technical Preview version 1904. The following new tiles on this dashboard help you evaluate readiness:

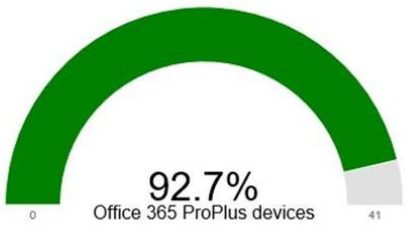
- Deployment
- Macro advisories
- Top add-ins by count of version

In the Configuration Manager console, go to the **Software Library** workspace, expand **Office 365 Client Management**, and select the **Office 365 ProPlus Upgrade Readiness** node.

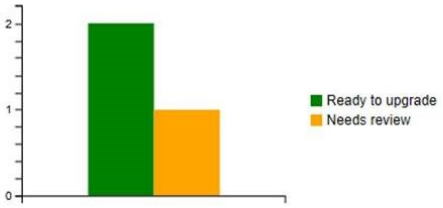
Office 365 Proplus Upgrade Readiness

Collection: All Systems Browse Target Office Architecture: 32-bit

Deployment



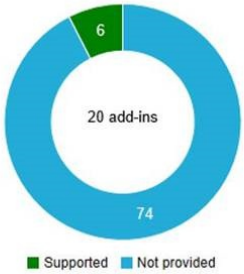
Device Readiness



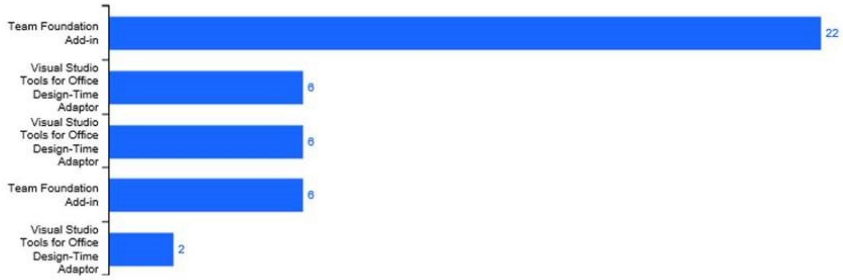
Learn more about this readiness data and how to do a macro assessment

Add-in readiness

Add-in support statements



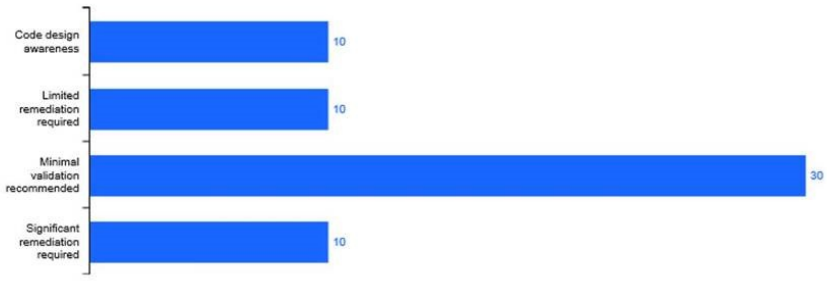
Top add-ins by version count



Devices with macros

Macro readiness

Macro advisories



For more information on prerequisites and using this data, see Integration for Office 365 ProPlus readiness.

Next steps

For more information about installing or updating the technical preview branch, see Technical preview.

For more information about the different branches of Configuration Manager, see Which branch of Configuration Manager should I use?

Features in Configuration Manager technical preview version 1906

6/12/2019 • 19 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Technical Preview)

This article introduces the features that are available in the technical preview for Configuration Manager, version 1906. Install this version to update and add new features to your technical preview site.

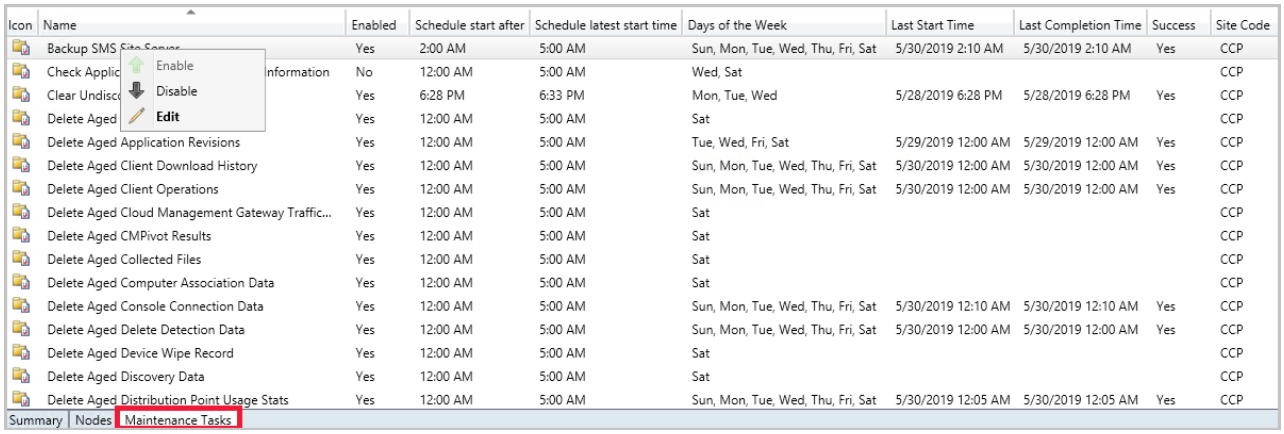
Review the technical preview article before installing this update. That article familiarizes you with the general requirements and limitations for using a technical preview, how to update between versions, and how to provide feedback.

The following sections describe the new features to try out in this version:

Improvements to maintenance tasks

Site server maintenance tasks can now be viewed and edited from their own tab on the details view of a site server. The new **Maintenance Tasks** tab gives you information such as:

- If the task is enabled
- The task schedule
- Last start time
- Last completion time
- If the task completed successfully



Icon	Name	Enabled	Schedule start after	Schedule latest start time	Days of the Week	Last Start Time	Last Completion Time	Success	Site Code
	Backup SMS	Yes	2:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat	5/30/2019 2:10 AM	5/30/2019 2:10 AM	Yes	CCP
	Check Applic	No	12:00 AM	5:00 AM	Wed, Sat				CCP
	Clear Undisc	Yes	6:28 PM	6:33 PM	Mon, Tue, Wed	5/28/2019 6:28 PM	5/28/2019 6:28 PM	Yes	CCP
	Delete Aged	Yes	12:00 AM	5:00 AM	Sat				CCP
	Delete Aged Application Revisions	Yes	12:00 AM	5:00 AM	Tue, Wed, Fri, Sat	5/29/2019 12:00 AM	5/29/2019 12:00 AM	Yes	CCP
	Delete Aged Client Download History	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat	5/30/2019 12:00 AM	5/30/2019 12:00 AM	Yes	CCP
	Delete Aged Client Operations	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat	5/30/2019 12:00 AM	5/30/2019 12:00 AM	Yes	CCP
	Delete Aged Cloud Management Gateway Traffic...	Yes	12:00 AM	5:00 AM	Sat				CCP
	Delete Aged CMPivot Results	Yes	12:00 AM	5:00 AM	Sat				CCP
	Delete Aged Collected Files	Yes	12:00 AM	5:00 AM	Sat				CCP
	Delete Aged Computer Association Data	Yes	12:00 AM	5:00 AM	Sat				CCP
	Delete Aged Console Connection Data	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat	5/30/2019 12:10 AM	5/30/2019 12:10 AM	Yes	CCP
	Delete Aged Delete Detection Data	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat	5/30/2019 12:00 AM	5/30/2019 12:00 AM	Yes	CCP
	Delete Aged Device Wipe Record	Yes	12:00 AM	5:00 AM	Sat				CCP
	Delete Aged Discovery Data	Yes	12:00 AM	5:00 AM	Sat				CCP
	Delete Aged Distribution Point Usage Stats	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat	5/30/2019 12:05 AM	5/30/2019 12:05 AM	Yes	CCP

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

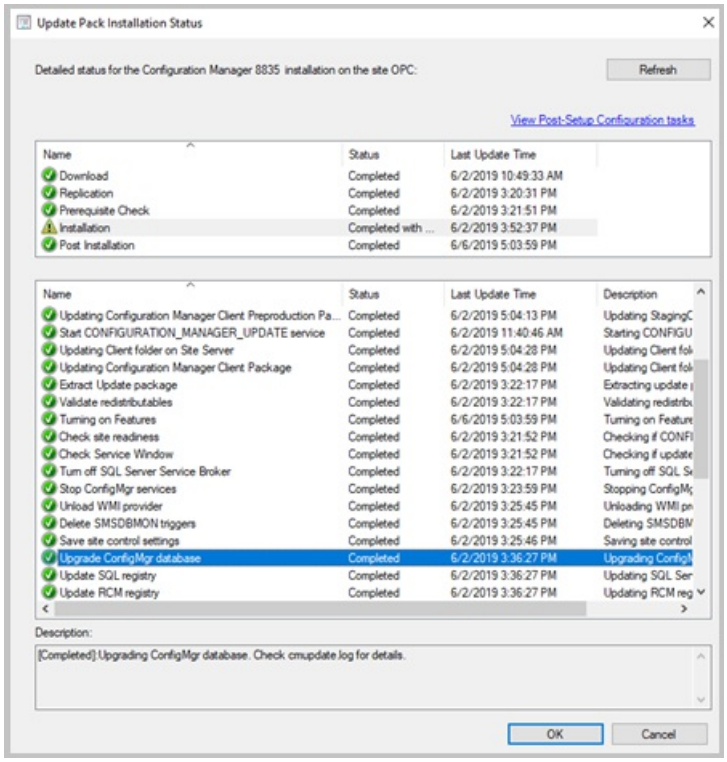
Edit a site maintenance task

1. In the **Administration** node, expand **Site Configuration**, then click on **Sites**.
2. Select a site from your list, then click on the **Maintenance Tasks** tab in the detail panel.
3. Right-click one of the maintenance tasks and select one of the following options:
   - **Enable** - Turn on the task.
   - **Disable** - Turn off the task.
   - **Edit** - Edit the task schedule or its properties.

Configuration Manager update database upgrade monitoring

When applying a Configuration Manager update, you can now see the state of the **Upgrade ConfigMgr database** task in the installation status window.

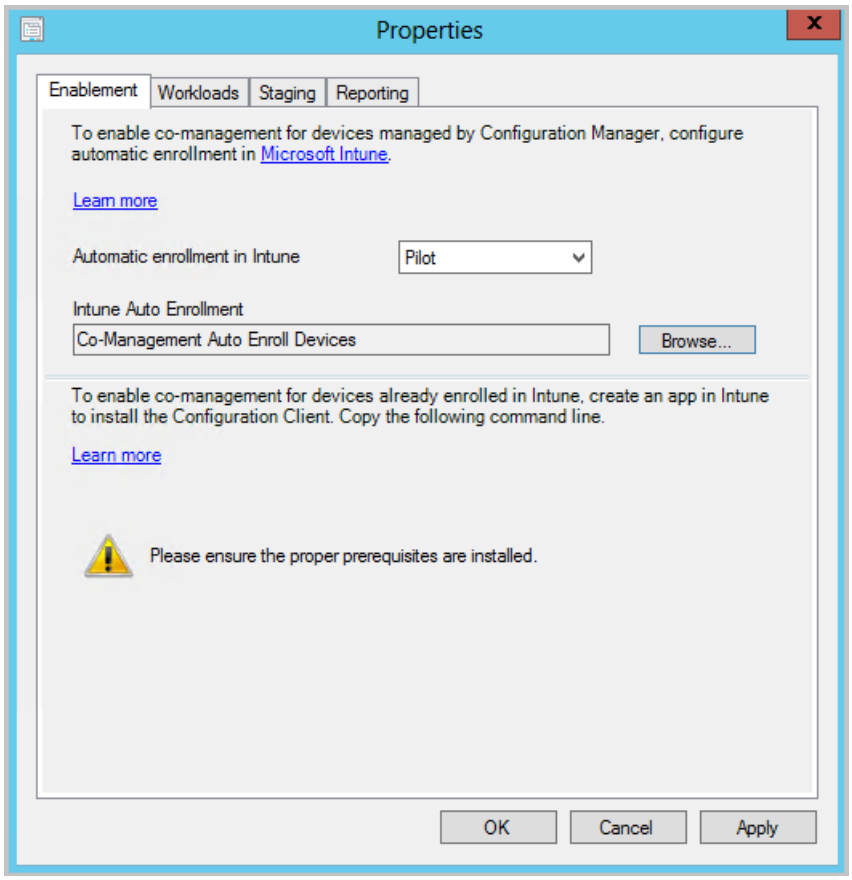
- If the database upgrade is blocked, then you'll be given the warning **In progress, needs attention**.
  - The cmupdate.log will log the program name and sessionid from SQL that is blocking the database upgrade.
- When the database upgrade is no longer blocked, the status will be reset to **In progress** or **Complete**.
  - When the database upgrade is blocked, a check is done every 5 minutes to see if it's still blocked.



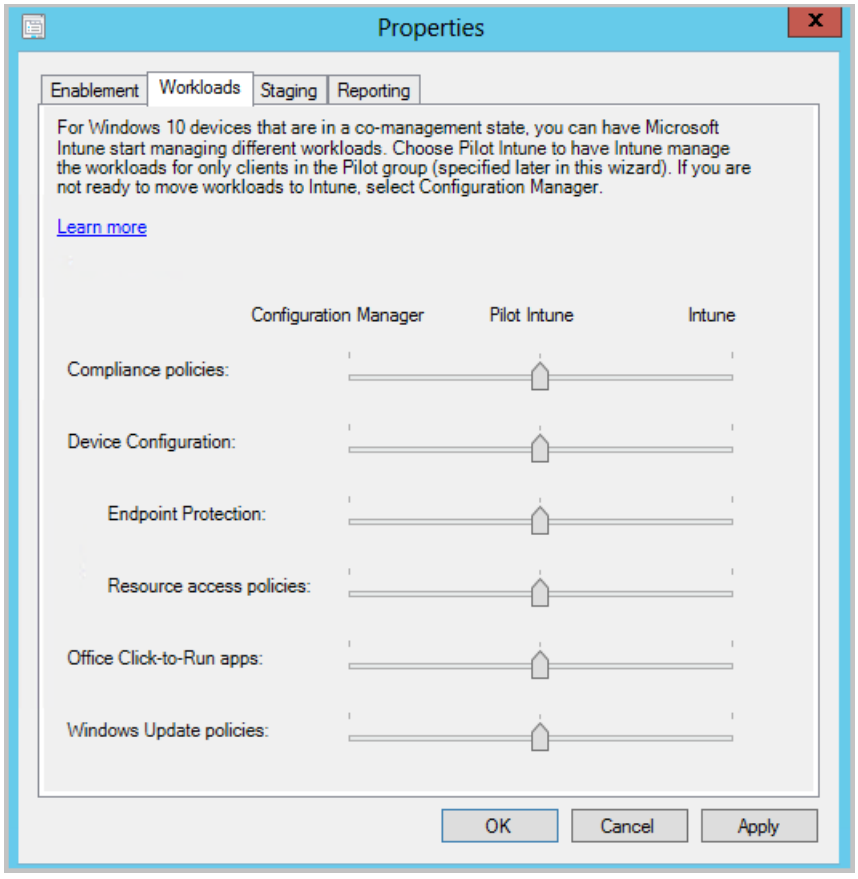
Multiple pilot groups for co-management workloads

You can now configure different pilot collections for each of the co-management workloads. Being able to use different pilot collections allows you to take a more granular approach when shifting workloads. This co-management change was made based on your product feedback.

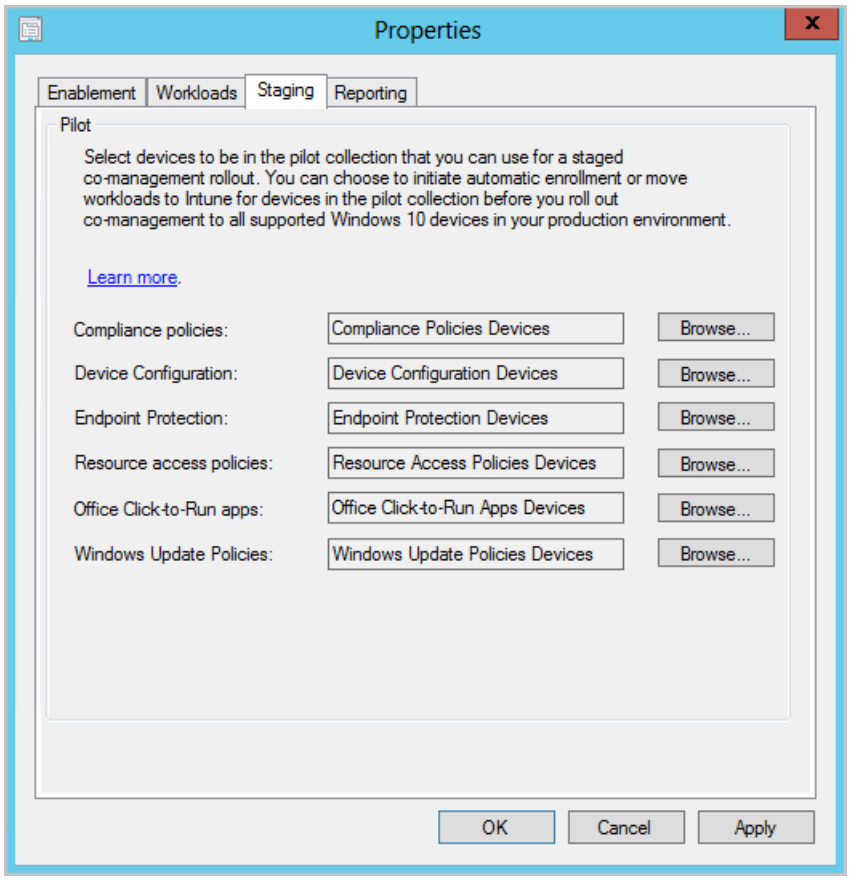
- In the **Enablement** tab, you can now specify an **Intune Auto Enrollment** collection.
  - The **Intune Auto Enrollment** collection should contain all of the clients you want to onboard into co-management. It's essentially a superset of all the other staging collections.



- The **Workloads** tab hasn't changed and you can still choose which workloads to transition.



- In the **Staging** tab, instead of using one pilot collection for all workloads, you can now choose an individual collection for each workload.



These options are also available when you first enable co-management.

Redesigned notification logic for newly available software

The **New Software is Available** notification will only show once for a user for a given application and revision. The user will no longer see the notification each time they log on. They'll only see another notification for an application if it has changed.

RBAC on Folders

Based on your UserVoice feedback you can now set security scopes on folders. If you have access to an object in the folder but don't have access to the folder, you'll be unable to see the object. Similarly, if you have access to a folder but not an object within it, you won't see that object.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the Configuration Manager console, right-click on a folder. For example, right-click a folder under the **Task Sequences** node.
2. Select **Folder** then **Set Security Scopes**.
3. Choose the security scopes you want to apply then click **OK**.

If you're already in the folder, you can also click on **Set Security Scopes** in the ribbon.

Azure Active Directory user group discovery

You can now discover user groups and members of those groups from Azure Active directory (Azure AD). Users found in Azure AD groups that haven't been previously discovered will be added as user resources in Configuration Manager. A user group resource record is created when the group is a security group.

Prerequisites

- Cloud Management Azure service
- Permission to read and search Azure AD groups

Limitations

Delta discovery for Azure Active Directory user group discovery is currently disabled.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. Go to the **Administration** workspace, expand **Cloud Services**, then click on the **Azure Services** node.
2. Select one of your Azure services, then click **Properties** in the ribbon.
3. In the **Discovery** tab, check the box for **Enable Azure Active Directory Group Discovery**, then click **Settings**.
4. Click **Add** under the **Discovery Scopes** tab.
   - You can modify the **Polling Schedule** in the other tab.
5. Select one or more user groups. You can **Search** by name and choose if you want to see **Security groups only**.
   - You'll be prompted to sign in to Azure when you click **Search** the first time.
6. Click **OK** when you're finished selecting groups.
7. Once discovery finishes running, browse your Azure AD user groups in the **Users** node.

When you onboard the cloud management service, you're given the option to configure Azure AD user group discovery.

Remote control anywhere using Cloud Management Gateway

An admin or helpdesk operator can now connect to a client via remote control over the Internet via cloud management gateway.

Prerequisites

- **Remote control user requirements:**
  - The Azure Active Directory (Azure AD) user needs to be discovered by Configuration Manager.
  - The user needs to be a permitted viewer for remote control under the **Remote Tools** page in the **Client Settings**.
- **Remote control client requirements:**
  - Remote control needs to be enabled under the **Remote Tools** page in the **Client Settings**.
  - The client needs to be upgraded to the latest version.
  - The client needs to be online from the Cloud Management Gateway

Known issues

For internet clients communicating with Cloud Management Gateway using Azure AD authentication, remote control may not work as expected.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

Connect to a client from the console

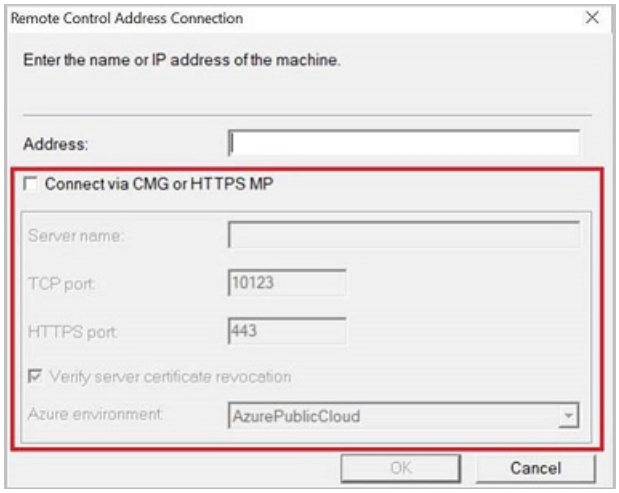
1. Choose a client that is communicating via CMG using a client PKI certificate. Make sure the client is online from the admin console.
2. Launch the remote control viewer from the console by right-clicking on a client, selecting **Start**, then **Remote Control**.

Use the standalone remote control viewer

1. Launch the standalone remote control viewer from `adminconsole\bin\i386\CmRcViewer.exe`. The folder and

file are located where the admin console is installed.

2. From the **File** menu, click on **Connect** to open the connection dialog.
3. Fill in the following options:
   - **Address**: The target address of the client. To connect using CMG, you must use the FQDN. You can't use the hostname or IP address.
     - For the **Try it out!** scenario, choose a client that is communicating via CMG using a client PKI certificate. Make sure the client is online from the admin console.
   - **Connect via CMG or HTTPs MP**: This option allows for fallback from a TCP direct connection to use the CMG service.
   - **Server name**: The CMG service name to which the current user and target client can connect.
   - **TCP port**: If needed, change the default port from 10123.
   - **HTTPS port**: If needed, change the default port from 443.
   - **Verify server certificate revocation**: If the CRL DP location isn't accessible for the current user, disable this option for testing purposes.
   - **Azure environment**: This option will prompt for sign in with your Azure AD credentials. Then, select the Azure environment for that user.
4. Click **OK** to connect. Remote control will attempt a direct connection first, then fallback to CMG for connection.



Improvements to Community Hub

Aside from the existing support for scripts and reports, the Community Hub now supports the following objects:

- PowerShell Scripts
- Reports
- Task sequences
- Applications
- Configuration items

The hub allows sharing these objects, but doesn't share any package source content associated with the objects. For example, boot images, OS upgrade packages, or driver packages referenced by a task sequence aren't shared.

The hub currently doesn't support object dependencies. For example, if you share app A that is dependent upon app B, it only shares app A with the community. Similarly, if a task sequence includes the Install Application step, the referenced apps aren't shared.

Passwords or other secrets are removed from a task sequence before sharing.

Updating Hub objects

The hub now manages updates to shared objects. There are two use cases for this scenario:

- You've downloaded an object from the hub. When you visit its entry in the Community Hub, the hub detects that you have an older version of the object. You can update it in your site with the latest version from the hub
- You created an object in your site, and share it in the hub. You then revise it in your site. When you revisit My Hub, because the version changed, you can update the object in the hub.
- Only the original contributor to the object uploaded to the hub can make changes and update their own item.

> **NOTE**
>
> The following prerequisites for Community Hub were recently updated in the 1904 Technical Preview documentation:
>
> - To download reports, you'll need **Full Administrator** rights in Configuration Manager.
> - To download reports, you need to turn on the option **Use Configuration Manager-generated certificates for HTTP site systems** at the site you're importing into. For more information, see enhanced HTTP. This prerequisite is also needed in 1906 Technical Preview for updating hub objects.

Known issues

When clicking on a report folder, the console may crash. To work around this issue, select the **Reports** node above the report folders, then filter or sort for the report.

For more information on Community Hub, including setup prerequisites and necessary permissions, see Community hub and GitHub.

Add joins, additional operators, and aggregators in CMPivot

Based on your UserVoice feedback for CMPivot, you now have additional arithmetic operators, aggregators, and the ability to add query joins such as using Registry and File together. The following items have been added:

Table operators

TABLE OPERATORS	DESCRIPTION
join	Merge the rows of two tables to form a new table by matching row for the same device
render	Renders results as graphical output

The render operator already exists in CMPivot. Support for multiple series and the **with** statement were added. For more information, see the examples section and Kusto's join operator article.

Limitations for joins

1. The join column is always implicitly done on the **Device** field.
2. You can use a maximum of 5 joins per query.
3. You can use a maximum of 64 combined columns.

Scalar operators

OPERATOR	DESCRIPTION	EXAMPLE
+	Add	`2 + 1, now() + 1d`

OPERATOR	DESCRIPTION	EXAMPLE
-	Subtract	`2 - 1, now() - 1d`
*	Multiply	`2 * 2`
/	Divide	`2 / 1`
%	Modulo	`2 % 1`

Aggregation functions

FUNCTION	DESCRIPTION
percentile()	Returns an estimate for the specified nearest-rank percentile of the population defined by Expr
sumif()	Returns a sum of Expr for which Predicate evaluates to true

Scalar functions

FUNCTION	DESCRIPTION
case()	Evaluates a list of predicates and returns the first result expression whose predicate is satisfied
iff()	Evaluates the first argument and returns the value of either the second or third arguments depending on whether the predicate evaluated to true (second) or false (third)
indexof()	Function reports the zero-based index of the first occurrence of a specified string within input string
strcat()	Concatenates between 1 and 64 arguments
strlen()	Returns the length, in characters, of the input string
substring()	Extracts a substring from a source string starting from some index to the end of the string
tostring()	Converts input to a string operation

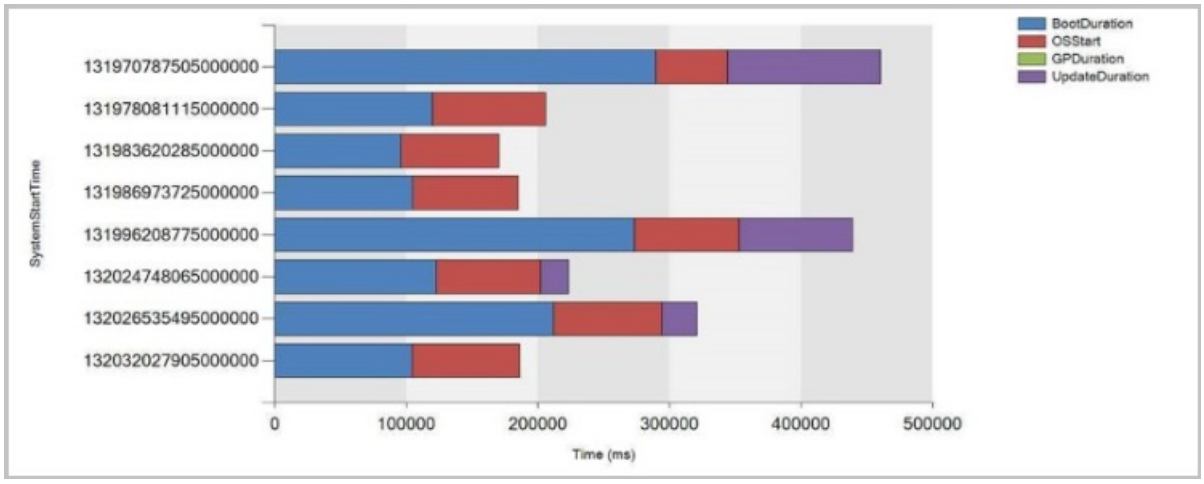
Examples

- Show device, manufacturer, model, and OSVersion:

```
ComputerSystem
| project Device, Manufacturer, Model
| join (OperatingSystem | project Device, OSVersion=Caption)
```

- Show graph of boot times for a device:

```
SystemBootData
| where Device == 'MyDevice'
| project SystemStartTime, BootDuration, OSStart=EventLogStart, GPDuration, UpdateDuration
| order by SystemStartTime desc
| render barchart with (kind=stacked, title='Boot times for MyDevice', ytitle='Time (ms)')
```



Improvements to CMPivot

To enable more people, such as security admins, to use CMPivot, we've expanded the ability for CMPivot to be run outside the console. We've also expanded the Security Admin role's default permissions. These changes give you the benefits of real-time queries across the organization.

Connect to CMPivot Standalone without using the command line.

- When you run CMPivot standalone, you'll be given a site connection prompt.
- You'll find the CMPivot app in the following path: `<site install path>\tools\CMPivot\CMPivot.exe`. You can run it from that path, or copy the entire CMPivot folder to another location.

Added CMPivot permissions to the Security Administrator role

The following permissions have been added to Configuration Manager's built-in **Security Administrator** role:

- Read on SMS Script
- Run CMPivot on Collection
- Read on Inventory Report

Improvements to Configuration Manager console

You can now enable some nodes of the Configuration Manager console to use the administration service. This change allows the console to communicate with the SMS Provider over HTTPS instead of via WMI.

In this version, it only affects the following nodes under the **Security** node in the **Administration** workspace:

- Administrative Users
- Security Roles
- Security Scopes
- Console Connections

Prerequisite

Enable the administration service. For more information, see Administration service.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. In the ribbon, select **Hierarchy Settings**.

2. On the **General** page, select the option to **Enable the Configuration Manager console to use the administration service**.

Support for Windows Virtual Desktop

Windows Virtual Desktop is a preview feature of Microsoft Azure and Microsoft 365. You can now use Configuration Manager technical preview to manage these virtual devices running Windows in Azure.

Similar to a terminal server, these virtual devices allow multiple concurrent active user sessions. To help with client performance, Configuration Manager now disables user policies on any device that allows these multiple user sessions. Even if you enable user policies, the client disables them by default on these devices, which include Windows Virtual Desktop and terminal servers.

The client only disables user policy when it detects this type of device during a new installation. For an existing client of this type that you update to this version, the previous behavior persists. On an existing device, it configures the user policy setting even if it detects that the device allows multiple user sessions.

If you require user policy in this scenario, and accept any potential performance impact, use the Configuration Manager SDK with the SMS_PolicyAgentConfig server WMI class. Set the new `PolicyEnableUserPolicyOnTS` property to `true`.

More frequent countdown notifications for restarts

The following improvements have been made for computer restart notifications:

1. In **Client Settings** on the **Computer Restart** page, you can now **Specify the snooze duration for computer restart countdown notifications (hours)**.
   - The default value is 4 hours.
   - Your snooze duration value should be less than the temporary notification value minus the value for the notification the user cant dismiss.
2. The maximum value for **Display a temporary notification to the user that indicates the interval before the user is logged off or the computer restarts (minutes)** increased from 1440 minutes (24 hours) to 20160 minutes (two weeks).
3. The user won't see a progress bar in the restart notification until the pending restart is less than 24 hours away.

Co-management auto-enrollment using device token

A new co-managed device now automatically enrolls to the Microsoft Intune service based on its Azure Active Directory (Azure AD) device token. It doesn't need to wait for a user to sign in to the device for auto-enrollment to start. This change helps to reduce the number of devices with the enrollment status *Pending user sign in*.

To support this behavior, clients need to be running Windows 10 version 1803 or later.

If the device token fails, it falls back to previous behavior with the user token. Look in the **ComanagementHandler.log** for the following entry:

```
Enrolling device with RegisterDeviceWithManagementUsingAADDeviceCredentials
```

Additional options for third-party update catalogs

You now have additional configuration options for how third-party update catalogs are synchronized into Configuration Manager.

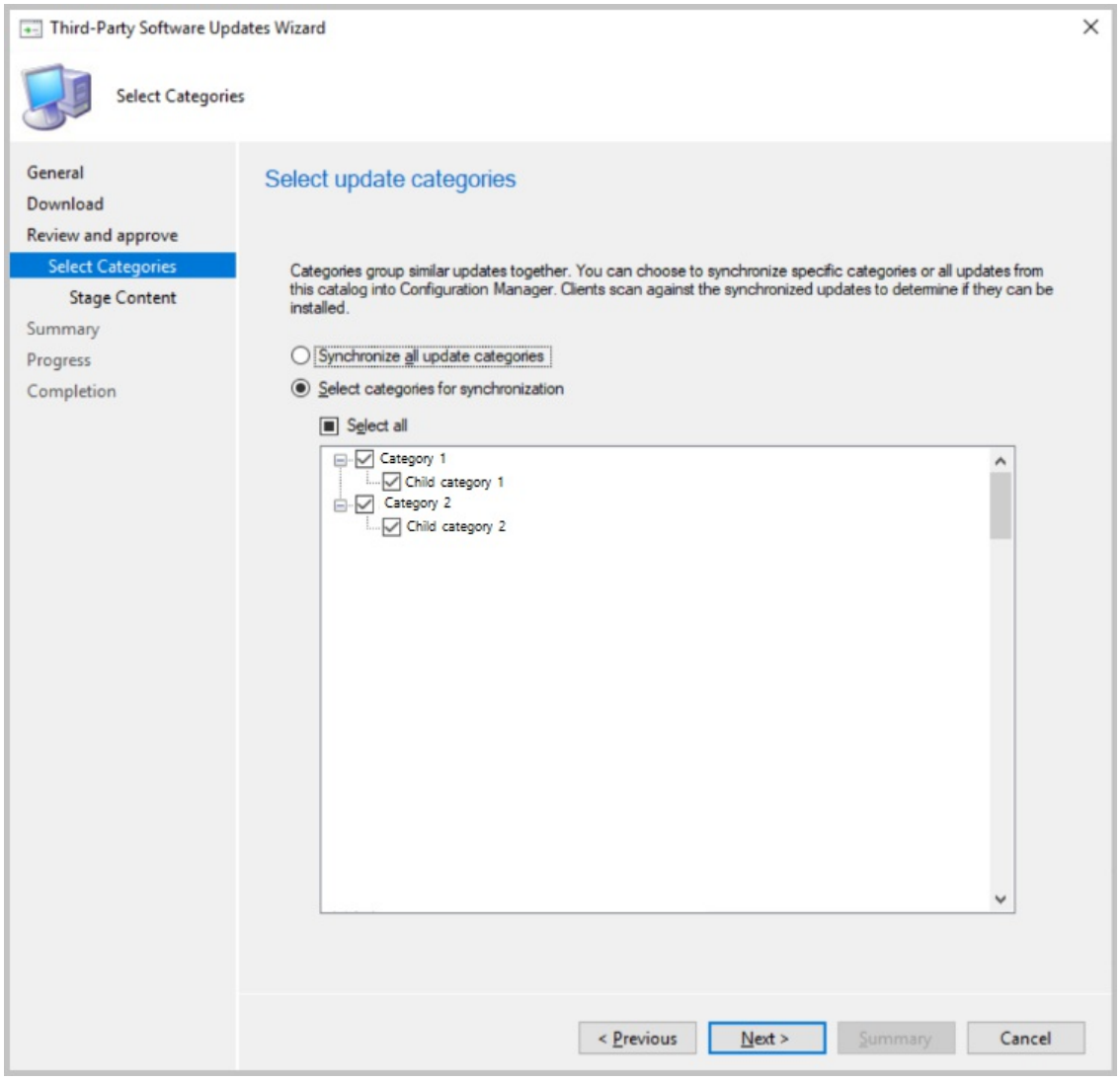
> **IMPORTANT**
>
> These options are only available for v3 third-party update catalogs, which support categories for updates. These options are disabled for catalogs that aren't published in the new v3 format.

Prerequisites

Enable third-party updates

New subscription to a third-party catalog

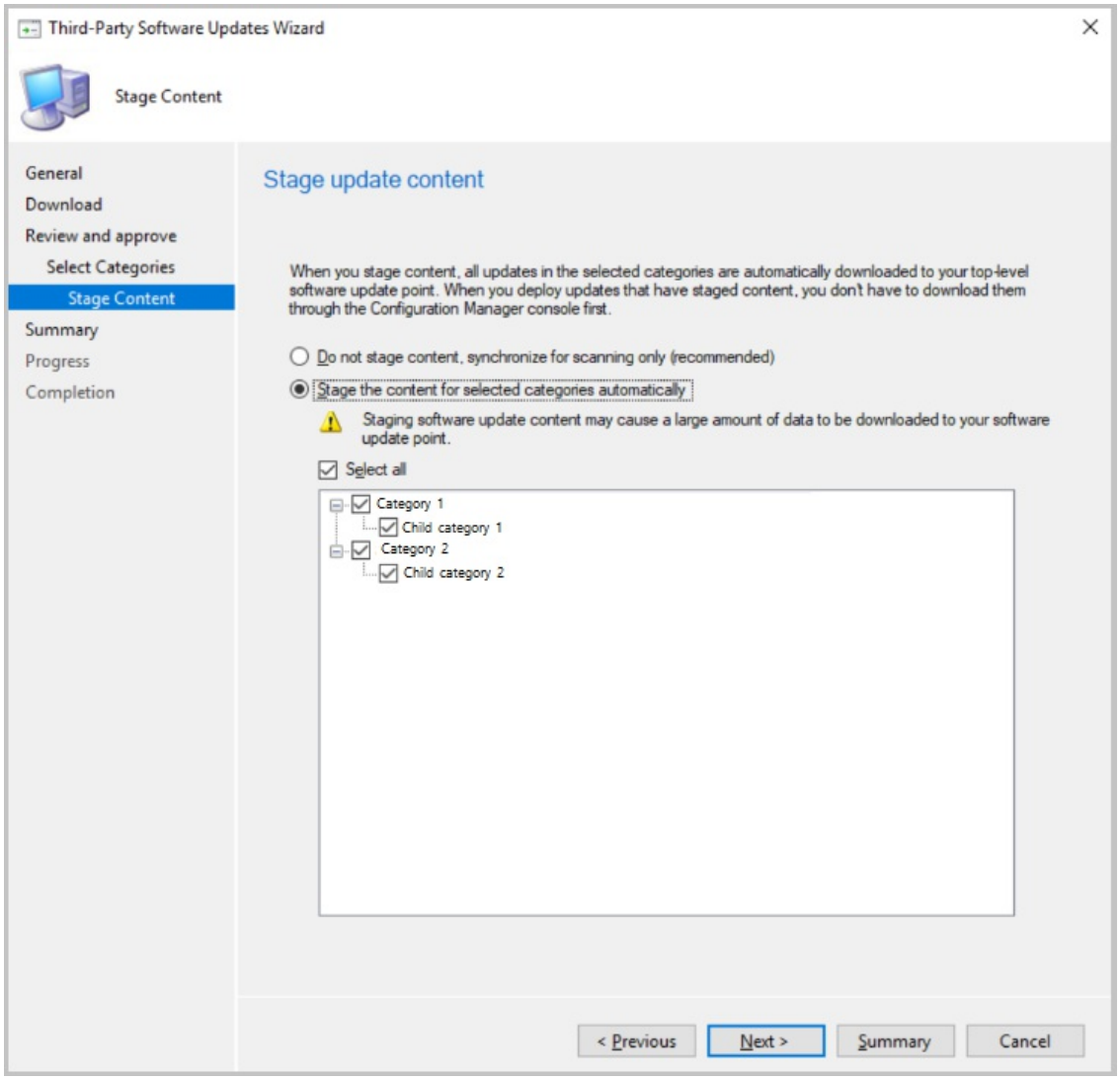
1. In the Configuration Manager console, go to the **Software Library** workspace. Expand **Software Updates** and select the **Third-Party Software Update Catalogs** node.
2. Select the catalog to subscribe and click **Subscribe to Catalog** in the ribbon.
3. Choose your options on the **Select Categories** page:
   - **Synchronize all update categories** (default)
     - Synchronizes all updates in the third-party update catalog into Configuration Manager.
   - **Select categories for synchronization**
     - Choose which categories and child categories to synchronize into Configuration Manager.



4. Choose if you want to **Stage update content** for the catalog. When you stage the content, all updates in the selected categories are automatically downloaded to your top-level software update point meaning you don't need to ensure they're already downloaded before deploying. You should only automatically stage

content for updates you are likely to deploy them to avoid excessive bandwidth and storage requirements.

- **Do not stage content, synchronize for scanning only (recommended)**
  - Don't download any content for updates in the third-party catalog
- **Stage the content for selected categories automatically**
  - Choose the update categories that will automatically download content.
  - The content for updates in selected categories will be downloaded to the top-level software update point's WSUS content directory.



Edit an existing subscription

1. In the Configuration Manager console, go to the **Software Library** workspace. Expand **Software Updates** and select the **Third-Party Software Update Catalogs** node.
2. Right-click on the catalog and select **Properties**.
3. Choose your options on the **Select Categories** tab.
   - **Synchronize all update categories** (default)
     - Synchronizes all updates in the third-party update catalog into Configuration Manager.
   - **Select categories for synchronization**
     - Choose which categories and child categories to synchronize into Configuration Manager.
4. Choose your options for the **Stage update content** tab.
   - **Do not stage content, synchronize for scanning only (recommended)**
     - Don't download any content for updates in the third-party catalog
   - **Stage the content for selected categories automatically**

- Choose the update categories that will automatically download content.
- The content for updates in selected categories will be downloaded to the top-level software update point's WSUS content directory.

Known issues

Saving setting for v3 catalogs with large numbers of categories may take longer than expected. We're working on improving this issue.

Clear app content from client cache during task sequence

In the **Install Application** task sequence step, you can now delete the app content from the client cache after the step runs. This behavior is beneficial on devices with small hard drives or when installing lots of large apps in succession.

Prerequisite

Update the target client to the latest version to support this new feature.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. Edit an existing task sequence or create a new custom task sequence.
2. Add and configure the Install Application step.
3. On the step, enable the option to **Clear application content from cache after installing**.
4. Deploy the task sequence to the target client.

New Windows 10, version 1903 and later product category

Windows 10, version 1903 and later was added to Microsoft Update as its own product rather than being part of the **Windows 10** product like earlier versions. This change caused you to do a number of manual steps to ensure that your clients see these updates. We've helped reduce the number of manual steps you have to take for the new product.

When you update to 1906 technical preview and have the **Windows 10** product selected for synchronization, the following actions occur automatically:

- The **Windows 10, version 1903 and later** product is added for synchronization.
- Automatic Deployment Rules containing the **Windows 10** product will be updated to include **Windows 10, version 1903 and later**.
- Servicing plans are updated to include the **Windows 10, version 1903 and later** product.

Management insights rule for NTLM fallback

Management insights includes a new rule that detects if you enabled the less secure NTLM authentication fallback method for the site: **NTLM fallback is enabled**.

When using the client push method of installing the Configuration Manager client, the site can require Kerberos mutual authentication. This enhancement helps to secure the communication between the server and the client. For more information, see How to install clients with client push.

Filter applications deployed to devices

Based on your UserVoice feedback, user categories for device-targeted application deployments now show as filters in Software Center.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. Specify a **user category** for an application on the **Software Center** page of its properties. For more information, see Manually specify application information.
2. Deploy the application to a machine as available.

Then open the app in Software Center and look at the available filters. For more information, see Applications in Software Center.

Known issue

If you *rename* an existing user category, it doesn't update on the client.

After adding a category to multiple apps, if you rename the category for one app, the renamed category only applies to that app. This change doesn't apply to other apps that reference the category. In Software Center, the renamed category shows as a new filter. The old category also shows as a filter.

To work around this issue, after you rename the category, deselect it on the app. Apply the changes, and then reselect the renamed category. This action revises the app, which applies the change.

Improvements to OS deployment

This version includes the following improvements to OS deployment:

- Based on your UserVoice feedback, it's now easier to edit variables when you run a task sequence. After you select a task sequence in the Task Sequence Wizard window, the page to edit task sequence variables includes an **Edit** button. You can use accessible keyboard shortcuts to edit the variables. This change helps in cases where a mouse isn't available.
- Based on your UserVoice feedback, the task sequence sets a new read-only variable **_SMSTSLastContentDownloadLocation**. This variable contains the last location where the task sequence downloaded or attempted to download content. Inspect this variable instead of parsing the client logs.
- This release further iterates on the improvement to the Disable BitLocker step from technical preview version 1905. It resolves the known issue with the client-side functionality, and adds a new variable, **OSDBitLockerRebootCountOverride**. Set this value from 0 to 15, and it overrides the count set by the step or the OSDBitlockerRebootCount variable. While the other methods only accept values 1 to 15, if you set this variable to 0, BitLocker remains disabled indefinitely. This new variable is useful when the task sequence sets one value, but you want to set a separate value on a per-device or per-collection basis.

Direct link to custom tabs in Software Center

You can now provide users with a direct link to a custom tab in Software Center.

Use the following URL format to open Software Center to a particular tab:

```
softwarecenter:page=CustomTab1
```

The string `CustomTab1` is the first custom tab in order.

For example, type this URL in the Windows **Run** window.

You can also use this syntax to open default tabs in Software Center:

COMMAND LINE	TAB
`AvailableSoftware`	Applications

COMMAND LINE	TAB
`Updates`	Updates
`OSD`	Operating Systems
`InstallationStatus`	Installation status
`Compliance`	Device compliance
`Options`	Options

Next steps

For more information about installing or updating the technical preview branch, see Technical preview.

For more information about the different branches of Configuration Manager, see Which branch of Configuration Manager should I use?

Features in Configuration Manager technical preview version 1905

5/21/2019 • 26 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Technical Preview)

This article introduces the features that are available in the technical preview for Configuration Manager, version 1905. Install this version to update and add new features to your technical preview site.

Review the technical preview article before installing this update. That article familiarizes you with the general requirements and limitations for using a technical preview, how to update between versions, and how to provide feedback.

The following sections describe the new features to try out in this version:

Improved control over WSUS Maintenance

You now have more granular control over the WSUS maintenance tasks that Configuration Manager runs to maintain healthy software update points. In addition to declining expired updates in WSUS, Configuration Manager can now remove obsolete updates from the WSUS database. The WSUS maintenance occurs after every synchronization.

Permissions

When the WSUS database is on a remote SQL server, the site server's computer account needs the following SQL permissions:

- The `db_datareader` and `db_datawriter` fixed database roles. For more information, see Database-Level Roles.
- The `CONNECT SQL` server permission must be granted to the site server's computer account. For more information, see GRANT Server Permissions (Transact-SQL).

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the Configuration Manager console, navigate to **Administration** > **Overview** > **Site Configuration** > **Sites**.
2. Select the site at the top of your Configuration Manager hierarchy.
3. Click **Configure Site Components** in the Settings group, and then click **Software Update Point** to open Software Update Point Component Properties.
4. In the **WSUS Maintenance** tab, select **Remove obsolete updates from the WSUS database**.

The obsolete update removal will be allowed to run for a maximum of 30 minutes before being stopped. It will start up again after the next synchronization occurs.

Improvements to Configuration Manager console

Based on customer feedback at the Midwest Management Summit (MMS) 2019, this release includes the following improvements to the Configuration Manager console:

Collections tab in devices node

In the **Assets and Compliance** workspace, go to the **Devices** node, and select a device. In the details pane, switch

to the new **Collections** tab. This tab lists the collections that include this device.

> **NOTE**
> This tab currently isn't available from a devices subnode under the **Device Collections** node. For example, when you select the option to **Show Members** on a collection.

Task sequences tab in applications node

In the **Software Library** workspace, expand **Application Management**, go to the **Applications** node, and select an application. In the details pane, switch to the new **Task sequences** tab. This tab lists the task sequences that reference this application.

Show collection name for scripts

In the **Monitoring** workspace, select the **Script Status** node. It now lists the **Collection Name** in addition to the ID.

Real-time actions from device lists

There are various ways to display a list of devices under the **Devices** node in the **Assets and Compliance** workspace.

- In the **Assets and Compliance** workspace, select the **Device Collections** node. Select a device collection, and choose the action to **Show members**. This action opens a subnode of the **Devices** node with a device list for that collection.
  - When you select the collection subnode, you can now start **CMPivot** from the Collection group of the ribbon.
- In the **Monitoring** workspace, select the **Deployments** node. Select a deployment, and choose the **View Status** action in the ribbon. In the deployment status pane, double-click the total assets to drill-through to a device list.
  - When you select a device in this list, you can now start **CMPivot** and **Run Scripts** from the Device group of the ribbon.

Multiselect and delete packages

In the **Software Library** workspace, expand **Application Management**, and select the **Packages** node. select more than one package. In the Package group of the ribbon, you can now delete more than one package at a time.

Order by program name in task sequence

In the **Software Library** workspace, expand **Operating Systems**, and select the **Task Sequences** node. Edit a task sequence, and select or add the Install Package step. If a package has more than one program, the drop-down list now sorts the programs alphabetically.

Correct names for client operations

In the **Monitoring** workspace, select **Client Operations**. The operation to **Switch to next Software Update Point** is now properly named.

Configure the default maximum run time for software updates

You can now specify the maximum amount of time a software update installation has to complete. You can specify the maximum run time for the following:

- **Feature updates** - An update that is in one of these three classifications:
  - Upgrades
  - Update rollups
  - Service packs
- **Non-feature updates** - An update that isn't a feature upgrade and whose product is listed as one of the

following:

- Windows 10 (all versions)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Office 365

All other products and classifications are not configurable with this setting. If you need to change the maximum run time of one of these updates, configure the software update settings

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the **Administration** workspace, expand **Site Configuration** and click on **Sites**.
2. Right-click on your top-level site, and select **Configure Site Components** then **Software Update Point**.
3. In the **Maximum Run Time** tab, modify the values for the following settings:
   - **Maximum run time for feature updates (minutes)**
   - **Maximum run time for non-feature updates (minutes**)

> **IMPORTANT**
> These settings only change the maximum runtime for new updates that are synchronized from Microsoft Update. It doesn't change the run time on existing feature or non-feature updates.

Known issue

This feature is listed in the **What's New** workspace of this technical preview version, but isn't available yet.

Windows Defender Application Guard file trust criteria

There's a new policy setting that enables users to trust files that normally open in Windows Defender Application Guard (WDAG). Upon successful completion, the files will open on the host device instead of in WDAG. For more information about the WDAG policies, see Configure Windows Defender Application Guard policy settings.

Prerequisites

- Clients running Windows 10 version 1809 or later

Permissions

- **Author Policy**, **Read**, **Run Report**, and **Modify Report** under **Settings for Windows Defender Application Guard**

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

Create a new WDAG policy

1. In the **Assets and Compliance** workspace, expand **Endpoint Protection**, then select the **Windows Defender Application Guard** node.
2. Select **Create Windows Defender Application Guard policy** in the ribbon.
3. In wizard, provide the **Name** for policy, and any other WDAG policies you need.
4. Under the **File Management** page, choose your option for **Allow users to trust files that open in Windows Defender Application Guard**.
   - **Prohibited:** Don't allow users to mark files as trusted (default).

- **File checked by antivirus:** Allow users to mark files as trusted after an antivirus check.
- **All files:** Allow users to mark any file as trusted.

5. Complete the wizard for additional policies, then select **Close** to exit the wizard once you're done.
6. Deploy the policy by selecting **Deploy** in the ribbon.

Edit an existing WDAG policy

1. In the **Assets and Compliance** workspace, expand **Endpoint Protection**, then select the **Windows Defender Application Guard** node.
2. Right-click on the policy you want to edit, then select **Properties**.
3. Switch to the **File Management** tab and choose your option for **Allow users to trust files that open in Windows Defender Application Guard**.
   - **Prohibited:** Don't allow users to mark files as trusted (default).
   - **File checked by antivirus:** Allow users to mark files as trusted after an antivirus check.
   - **All files:** Allow users to mark any file as trusted.
4. Select **OK** to save your selection and close the policy properties.
5. Deploy the policy by selecting **Deploy** in the ribbon.

Known issues

- In the client's DCMReporting.log, you may see errors logged which typically don't effect functionality:
  - On compatible devices:
    - FileTrustCriteria_condition not found
  - On non-compatible devices:
    - FileTrustCriteria_condition not found
    - FileTrustCriteria_could not be located in the map
    - FileTrustCriteria_condition not found in digest

Application groups

Create a group of applications that you can send to a user or device collection as a single deployment. The metadata you specify about the app group is seen in Software Center as a single entity. You can order the apps in the group so that the client installs them in a specific order.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the Configuration Manager console, go to the **Software Library** workspace. Expand **Application Management** and select the **Application Group** node.
2. On the **General Information** page, specify information about the app group.
3. On the **Software Center** page, include information that shows in Software Center.
4. On the **Application Group** page, select **Add**. Select one or more apps for this group. Reorder them using the **Move Up** and **Move Down** actions.
5. Complete the wizard.

Deploy the app group using the same process as for an application. For more information, see Deploy applications.

To troubleshoot an app group deployment, use the **AppGroupHandler.log** and **AppEnforce.log** files on the client.

Known issues

- Deploy the app group as required, without user interaction, and to a device collection.

- The app group isn't currently shown in Software Center.
- The deployment of an app group doesn't show in the **Deployments** node of the **Monitoring** workspace.

Task sequence as an app model deployment type

You can now install complex applications using task sequences via the application model. Add a deployment type to an app that's a task sequence, either to install or uninstall the app. This feature provides the following behaviors:

- Deploy an app task sequence to a user collection
- Display the app task sequence with an icon in Software Center. An icon makes it easier for users to find and identify the app task sequence.
- Define additional metadata for the app task sequence, including localized information

You can only add a non-OS deployment task sequence as a deployment type on an app. High-impact, OS deployment, or OS upgrade task sequences aren't supported. A user-targeted deployment still runs in the user context of the local System account.

Prerequisites

Create a custom task sequence:

- Use only non-OS deployment steps, for example: Install Application, Run Command Line, or Run PowerShell Script. For more information including the full list of supported steps, see Create a task sequence for non-OS deployments.
- On the task sequence properties, **User Notification** tab, don't select the option for a high-impact task sequence.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the Configuration Manager console, create an application. Use the option to **Manually specify the application information**.

   > **TIP**
   > You can also add this deployment type to an existing app.

2. When you add a deployment type, select **Task Sequence** from the list of Types.
3. On the Task Sequence page of the Create Deployment Type wizard, select an **Install task sequence**. Optionally, select an **Uninstall task sequence**.

   > **NOTE**
   > If your task sequence doesn't appear in the list, double-check that it doesn't include any OS deployment or OS upgrade steps. Also confirm that it isn't marked as a high-impact task sequence. For more information, see the Prerequisites.

4. Further configure the app and deployment type as necessary. For example, customize the icon on the Software Center tab of the app.
5. Deploy the app as usual.

Known issue

The client-side functionality isn't yet completed, so you won't see the deployment in Software Center.

BitLocker management

You can now use Configuration Manager to install and manage the Microsoft BitLocker Administration and Monitoring (MBAM) client.

For more information, see Microsoft expands BitLocker management capabilities for the enterprise.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace, expand **Endpoint Protection**, and select the **BitLocker Management (MBAM)** node.
2. In the ribbon, select the action to create a policy.
3. On the **General** page, specify a name and optional description. Select the components to enable on clients with this policy:
   - **Client Management**: Manage the key recovery service backup of BitLocker Drive Encryption recovery information
   - **Operating System Drive**: Manage whether the OS drive is encrypted
4. On the **Client Management** page, specify the following settings:
   - **Configure MBAM Services**: If you enable this setting, key recovery info is automatically and silently backed up to the Configuration Manager site.
   - **Select BitLocker recovery information to store**: Configure it to use a recovery password and key package, or just a recovery password.
   - **Enter client checking status frequency in (minutes)**: This value is the interval at which the MBAM client checks with the site for updated policy.
5. On the **Operating System Drive** page, specify the following settings:
   - **Operating System Drive Encryption Settings**: If you enable this setting, the user has to protect the OS drive, and BitLocker encrypts the drive. If you disable it, the user can't protect the drive.

     > **NOTE**
     > If the drive is already encrypted, and you disable this setting, BitLocker decrypts the drive.

   - **Allow BitLocker without a compatible TPM (requires a password)**
   - **Select protector for operating system drive**: Configure it to use a TPM and PIN, or just the TPM.
   - **Configure minimum PIN length for startup**: If you require a PIN, this value is the shortest length the user can specify. The user enters this PIN when the computer boots to unlock the drive.
6. Complete the wizard.
7. Deploy the policy to a device collection.

Monitor

Use the following logs to monitor and troubleshoot:

Client

- MBAM event log: in the Windows Event Viewer, browse to Applications and Services > Microsoft > Windows > MBAM
- **BitlockerMangementHandler.log** in client logs path, `%WINDIR%\CCM\Logs` by default

Management point

- MBAM Recovery Service event log
- MBAM Recovery Service trace logs:
  `<Default IIS Web Root>\Microsoft BitLocker Management Solution\Logs\Recovery And Hardware Service\trace*.etl`

Task sequence debugger

The task sequence debugger is a new troubleshooting tool. You deploy a task sequence in debug mode to a collection of one device. It lets you step through the task sequence in a controlled manner to aid troubleshooting and investigation.

Prerequisites

- Update the Configuration Manager client on the target device
- Update the boot image associated with the task sequence to make sure it has the latest client version

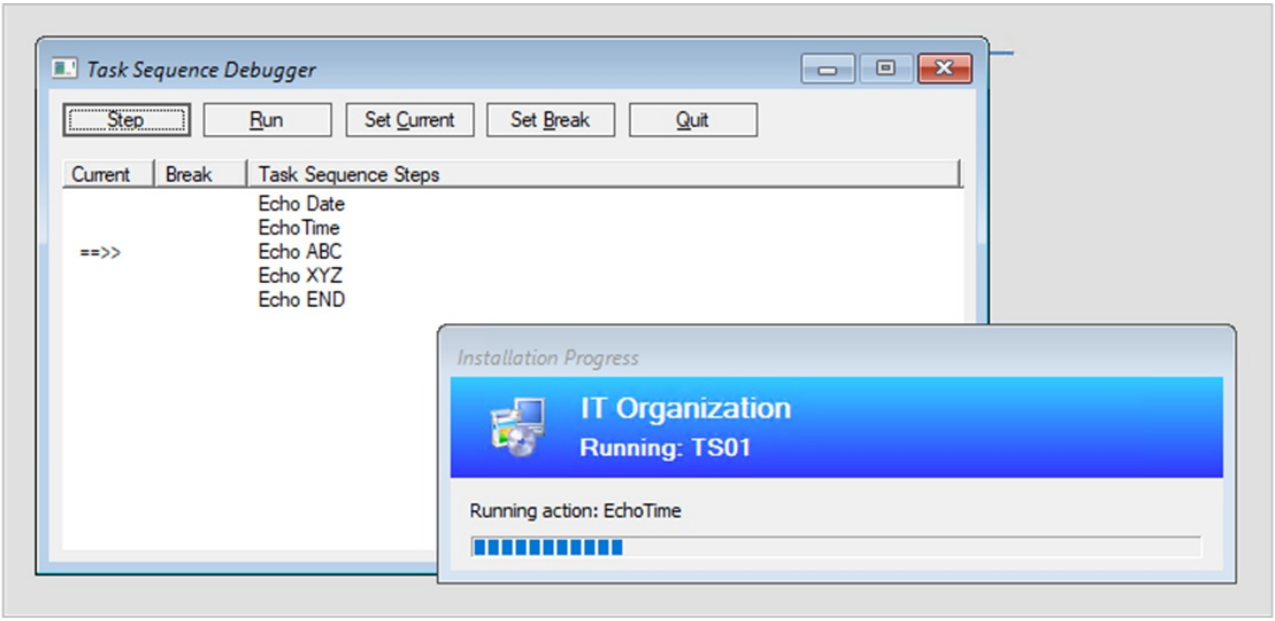
Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the Configuration Manager console, go to the **Software Library** workspace, expand **Operating Systems**, and select **Task Sequences**.
2. Select a task sequence. In the Deployment group of the ribbon, select **Debug**.

> **TIP**
> Alternatively, set the variable **TSDebugMode** to `TRUE` on a collection to which the task sequence is deployed. This variable changes the behavior of any task sequence on any device in that collection.

When the task sequence runs on the device in Windows PE, the Task Sequence Debugger window opens similar to the following screenshot:



The debugger includes the following controls:

- **Step**: From the *current* position, run only the next step in the task sequence.

- **Run**: From the *current* position, run the task sequence normally to the end or the next *break* point.
- **Set Current**: Select a step in the debugger and then select **Set Current**. This action moves the *current* pointer to that step. This action allows you to skip steps or move backwards.

  > **WARNING**
  > The debugger doesn't consider the type of step when you change the current position in the sequence. Some steps may fail or cause significant damage to a device if run out of order. Use this option at your own risk.

- **Set Break**: Select a step in the debugger and then select **Set Break**. This action adds a *break* point in the debugger. When you **Run** the task sequence, it stops at a *break*.
- **Quit**: Quit the debugger and stop the task sequence.

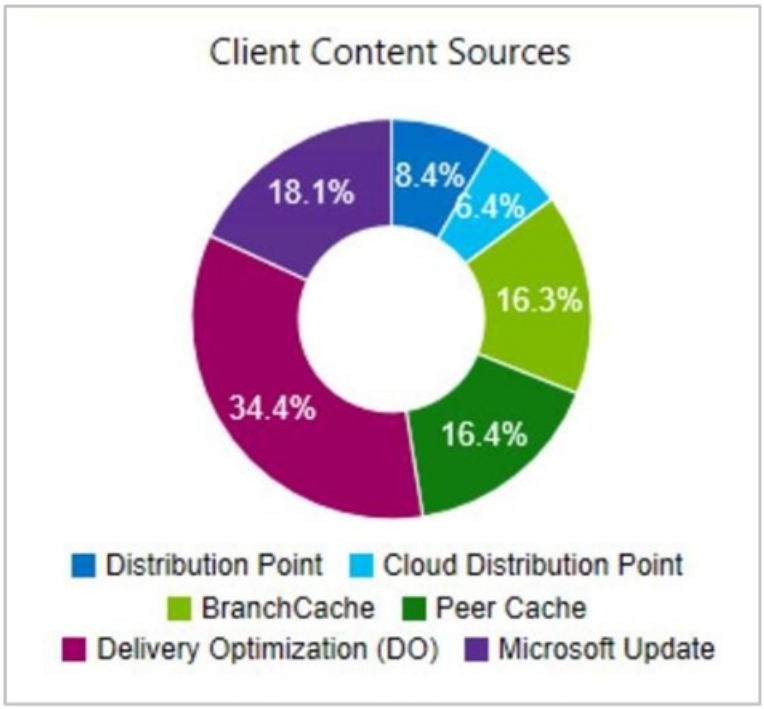
Known issues

The debugger currently only works in Windows PE.

Delivery Optimization in client data sources dashboard

The Client data sources dashboard now includes Delivery Optimization data. This dashboard helps you understand from where clients are getting content in your environment.

For example, the Client Content Sources tile displays the source from which clients got content:



To include Delivery Optimization on this dashboard, do the following actions:

- Configure the client setting, **Enable installation of Express Updates on clients** in the Software Updates group
- Deploy Windows 10 express updates

For more information, see Manage Express installation files for Windows 10 updates.

The dashboard also includes the **Microsoft Update** source. Devices report this source when the Configuration Manager client downloads software updates from Microsoft cloud services. These services include Microsoft Update and Office 365.

Improvements to Community Hub

Aside from the existing support for scripts and reports, the Community Hub now supports the following objects:

- Task sequences
- Applications
- Configuration items

The hub doesn't share any package source content associated with these objects. For example, boot images, OS upgrade packages, or driver packages referenced by a task sequence.

The hub currently doesn't support object dependencies. For example, if you share app A that is dependent upon app B, it only shares app A with the community. Similarly, if a task sequence includes the Install Application step, the referenced apps aren't shared.

It removes any password or other secret from a task sequence before sharing.

For more information on Community Hub, including setup prerequisites and necessary permissions, see Community hub and GitHub.

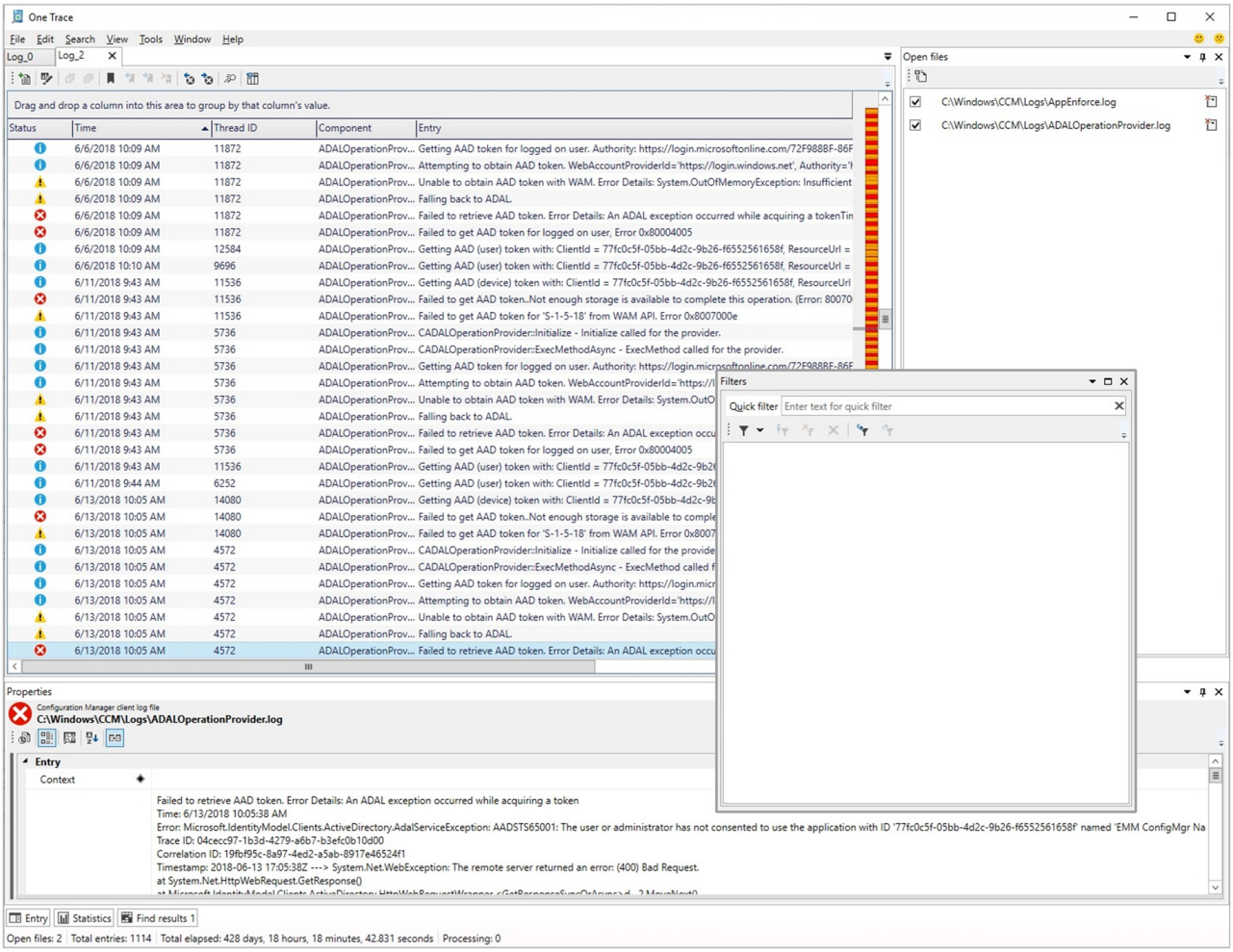
View SMBIOS GUID in device lists

In both the Devices and Device Collections nodes, you can now add a new column for **SMBIOS GUID**. This value is the same as the **BIOS GUID** property of the System Resource class. It's a unique identifier for the device hardware.

OneTrace log viewer

OneTrace is a new log viewer with Support Center. It works similarly to CMTrace, with the following improvements:

- A tabbed view
- Dockable windows
- Improved search capabilities
- Ability to enable filters without leaving the log view
- Scrollbar hints to quickly identify clusters of errors
- Fast log opening for large files



OneTrace works with many types of log files, such as:

- Configuration Manager client logs
- Configuration Manager server logs
- Status messages
- Windows Update ETW log file on Windows 10
- Windows Update log file on Windows 7 & Windows 8.1

Prerequisites

- .NET Framework version 4.6 or later

Install

Find the Support Center installer on the site server at the following path:
`cd.latest\SMSSETUP\Tools\SupportCenter\SupportCenterInstaller.msi`.

> **NOTE**
>
> Support Center and OneTrace use Windows Presentation Foundation (WPF). This component isn't available in Windows PE. Continue to use CMTrace in boot images with task sequence deployments.

Software Center infrastructure improvements

Software Center communicates with a management point for apps targeted to users as available. It doesn't use the application catalog anymore. This change makes it easier for you to remove the application catalog from the site.

Now in this release, the management point checks the health of its user service every five minutes. It reports any issues via status messages for the SMS_MP_CONTROL_MANAGER site component.

IMPORTANT

These iterative improvements to Software Center and the management point are to retire the application catalog roles. The Silverlight user experience isn't supported as of current branch version 1806. In the first current branch release after June 30, 2019, updated clients will automatically use the management point for user-available application deployments. You also won't be able to install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.

Improvements to Software Center tab customizations

You can now add up to five custom tabs in Software Center. You can also edit the order in which these tabs appear in Software Center.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

Add custom tabs

1. In the **Administration** workspace, go to the **Client Settings** mode.
2. Right-click on the **Default Client Settings** or one of your custom settings, then select **Properties**.
3. Go to the **Software Center** group and click on **Customize** to open the **Software Center Customization** window.
   - The **Customize** button is enabled once **Yes** is set for **Select these new settings to specify company information**.
4. Select **Tabs** from the tab control located at the top, then click **Add Tab**.
5. Type in your **Tab name** (maximum 20 characters), its **Content URL**, then **OK** when done.
6. Click **Add Custom Tab** and add a second custom tab.
7. Click **OK** in the **Software Center Customization** window, then **OK** on your settings window.
8. Observe the changes in **Software Center**.

Reorder custom tabs

1. In **Client Settings**, go to the ***Software Center** group and click on **Customize**.
2. Select a tab from the visible tabs list, then click either **Move Up** or **Move Down**.
3. Click **Ok**.
4. Observe the changes in **Software Center**.

Improvements to app approvals

This release includes the following improvements to app approvals:

NOTE

These improvements refer to the optional feature **Approve application requests for users per device**.

- If you approve an app request in the console, and then deny it, you can now approve it again. The app is reinstalled on the client after you approve it.
- There's a new WMI method, **DeleteInstance** to remove an app approval request. This action doesn't uninstall the app on the device. If it's not already installed, the user can't install the app from Software Center. The version 1810 blog post below includes a PowerShell script sample that you can adjust for use with this API.
- Call the **CreateApprovedRequest** API to create a pre-approved request for an app on a device. To prevent

automatically installing the app on the client, set the **AutoInstall** parameter to `FALSE`. The user sees the app in Software Center, but it's not automatically installed.

Other app approval resources

- Approve applications
- Application approval improvements in ConfigMgr 1810
- Updates to the application approval process in Configuration Manager

Retry the install of pre-approved applications

You can now retry the installation of an app that you previously approved for a user or device. The approval option is only for available deployments. If the user uninstalls the app, or if the initial install process fails, Configuration Manager doesn't reevaluate its state and reinstall it. This feature allows a support technician to quickly retry the app install for a user that calls for help.

Prerequisites

- Enable the optional feature **Approve application requests for users per device**.
- Deploy an app that requires approval, and approve it. For more information, see Approve applications.

  > **TIP**
  > Alternatively, use the other new feature in this technical preview version to Install applications for a device. It creates an approved request for the app on the device.

- Your user account needs the **Approve** permission on the Application object. For example, the **Application Administrator** or **Application Author** built-in roles have this permission.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. To test this feature, manually uninstall the app on the device.
2. In the Configuration Manager console, go to the **Software Library** workspace, expand **Application Management**, and select the **Approval Requests** node.
3. Select the previously approved app. In the Approval Request group of the ribbon, select **Retry install**.

Install applications for a device

From the Configuration Manager console, you can now install applications to a device in real time. This feature can help reduce the need for separate collections for every application.

Prerequisites

- Enable the optional feature **Approve application requests for users per device**.
- Deploy the application as available to the **All Systems** collection.
  - On the **Deployment Settings** page of the deployment wizard, select the following option: **An administrator must approve a request for this application on the device**.

> **NOTE**
> With these deployment settings, the app isn't shown as available in Software Center. A user can't install the app with this deployment. After you use this action to install the app, the user can run it, and see its installation status in Software Center.

- Your user account needs the following permissions:
  - Application: **Approve**
  - Collection: **View Collected File**

  For example, the **Application Administrator** built-in role has these permissions.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace, and select the **Devices** node. Select the target device, and then select the **Install application** action in the ribbon.
2. Select one or more applications from the list. The list only shows applications that you already deployed.

This action triggers the installation of the selected pre-deployed applications on the device.

To see status of the approval request, in the **Software Library** workspace, expand **Application Management**, and select the **Approval Requests** node. Monitor the app installation the same as usual in the **Deployments** node of the **Monitoring** workspace.

More frequent countdown notifications for restarts

End users will now be reminded more frequently of a pending restart with intermittent countdown notifications. The end user will be reminded about restarting their device every 4 hours until the final countdown notification occurs.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. Go to the **Client Settings** node under the **Administration** workspace.
2. Right-click on the client device settings to modify and select **Properties**, or create a new set of custom settings.
3. On the **Computer Restart** page, set the following values:
   - **Display a temporary notification to the user that indicates the interval before the user is logged off or the computer restarts (minutes)** - Indicates the total time given to users to restart the device after software enforcement. The value should be greater than 240 minutes (4 hours) and at least 4 hours greater than the setting for the dialog the user can't close.
     - If the user closes or clicks **Snooze** on the restart notification from the dialog window, the snooze interval is 4 hours until the next temporary notification occurs.
     - When toast notifications are used and the user didn't click on it or notice it, the same toast notification will reoccur in 4 hours.
     - For more information on what a toast notification is, see Plan for Software Center
   - **Display a dialog box that the user cannot close, which displays the countdown interval before the user is logged off or the computer restarts (minutes)** - Indicates the time interval for the final countdown notification, which the user can't close.
     - For example, if the value is 60, the user will see a notification they can't close an hour before restart enforcement.
     - The final countdown notification will always be a dialog window with the **Snooze** button disabled.

- **When a deployment requires a restart, show a dialog window to the user instead of a toast notification**
  - **No** - Toast notifications are used to remind users of the time remaining before restart.
  - **Yes** - A more intrusive dialog window is used to remind the user of a pending restart.

4. Observe the restart notification behavior on a client after software enforcement. The settings above apply only when software has been installed at the deadline and requires a restart. If a user proactively installed the software before the deadline, they'll see different toast notifications and a different dialog for the restart.

Synchronize collection membership results to Azure Active Directory groups

You can now enable the synchronization of collection memberships to an Azure Active Directory (Azure AD) group. This synchronization allows you to use your existing on premises grouping rules in the cloud. You can synchronize device collections. Only Azure AD-joined devices are synchronized to Azure AD.

The Azure AD synchronization happens every five minutes. It's a one-way process, from Configuration Manager to Azure AD. Changes made in Azure AD aren't reflected in Configuration Manager collections, but aren't overwritten by Configuration Manager. For example, if the Configuration Manager collection has two devices, and the Azure AD group has three different devices, after synchronization the Azure AD group has five devices.

Prerequisites

- Cloud Management
- Azure Active Directory user discovery

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

Add group write permission to the app

1. Go to the **Azure Active Directory Tenants** node, select the web app for *Cloud Management*, and then select **Update Application Settings** in the ribbon.
2. Select **Yes** and you'll be given a sign in prompt for Azure.
3. Sign in with a user that has group write permission for Azure AD.
4. Once you successfully sign in, you'll see a dialog box that reads **Application settings successfully updated**.

Create collection Azure AD group mapping

1. Right-click on a collection and select the **Cloud Sync** tab.
2. Select **Add** to select Azure AD objects.
   - If you need to remove an Azure AD group, select it, then choose **Remove**.
3. Select your tenant then choose **Search**. You'll be prompted to sign in to Azure.
   - You can also type in a partial or full group name before clicking **Search**.
4. Once you sign in, select an *assigned* group from the populated search list, then select **OK**.
5. Select **Apply** to save the collection properties.

Limitations

Only one Azure AD tenant is supported. If you have more than one tenant, the results for collection membership synchronization to Azure AD are unpredictable.

Configure client cache minimum retention period

You can now specify the minimum time for the Configuration Manager client to keep cached content. This client setting controls how long the client stores content in the cache before deleting it.

In the **Client Cache settings** group of client settings, configure the following setting: **Minimum duration before**

cached content can be removed (minutes). By default this value is 1,440 minutes (24 hours).

This setting gives you greater control over the client cache on different types of devices. You might reduce the value on clients that have small hard drives and don't need to keep existing content before another deployment runs.

> **NOTE**
> In the same client setting group, the existing setting to **Enable Configuration Manager client in full OS to share content** is now renamed to **Enable as peer cache source**. The behavior of the setting doesn't change.

Improvements to OS deployment

This release includes the following improvements to OS deployment:

- Based on your UserVoice feedback, the Disable BitLocker task sequence step has a new restart counter. Use this option to specify the number of restarts to keep BitLocker disabled. Instead of adding multiple instances of this step, set a value between 1 (default) and 15. You can also set this behavior with the task sequence variable **OSDBitlockerRebootCount**.

  > **NOTE**
  > There is a known issue with the client-side functionality, so the task sequence only disables BitLocker for one restart.

- Technical preview version 1904 included a feature to Pre-cache driver packages and OS images. This version improves upon that functionality by also adding packages. Specify the architecture and language of the package on its properties.

Add a SQL AlwaysOn node

You can now add a new secondary replica node to an existing SQL AlwaysOn availability group. Instead of a manual process, use Configuration Manager setup to make this change:

1. Use the hierarchy maintenance tool to stop the site: `preinst.exe /stopsite`
2. Modify the availability group using SQL Server procedures:
   a. Create a backup of the site database from the primary replica.
   b. Restore that backup to the new secondary replica server.

   > **NOTE**
   > This process also works with removing a secondary replica node from a SQL AlwaysOn availability group. For more information, see Remove a secondary replica from an availability group.

3. Run Configuration Manager setup, and select the option to modify the site.
4. Specify the availability group listener name as the database name. If the listener uses a non-standard network port, specify that as well. This action causes setup to make sure each node is appropriately configured. It also starts a database recovery process.

For more information on Configuration Manager support for SQL AlwaysOn, see the following articles:

- Prepare to use SQL Server Always On availability groups
- Configure SQL Server Always On availability groups

Next steps

For more information about installing or updating the technical preview branch, see Technical preview.

For more information about the different branches of Configuration Manager, see Which branch of Configuration Manager should I use?

Migrate data between hierarchies in Configuration Manager

2/12/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use migration to transfer data from a supported source hierarchy to your Configuration Manager (current branch) destination hierarchy. When you migrate data from a source hierarchy:

- You access data from the site databases in the source infrastructure, and then transfer that data to your current environment.
- Migration doesn't change the data in the source hierarchy. Instead it discovers the data and stores a copy in the database of the destination hierarchy.

Consider the following points when you plan your migration strategy:

- You can migrate an existing Configuration Manager 2007 SP2 infrastructure to Configuration Manager (current branch).
- You can migrate some or all of the supported data from a source site.
- You can migrate the data from a single source site to several different sites in the destination hierarchy.
- You can move data from multiple source sites to a single site in the destination hierarchy.

The following video discusses and demonstrates two common migration scenarios. It also includes options for including Microsoft Azure in migration plans.

Concepts

Configuration Manager uses the following concepts and terms during migration.

Source hierarchy

A hierarchy that runs a supported version of Configuration Manager and has data that you want to migrate. When you set up migration, you identify the source hierarchy when you specify the top-level site of a source hierarchy. After you specify a source hierarchy, the top-level site of the destination hierarchy gathers data from the database of the designated source site to identify the data that you can migrate.

For more information, see Source hierarchies.

Source sites

The sites in the source hierarchy that have data that you can migrate to your destination hierarchy.

For more information, see Source sites.

Destination hierarchy

A Configuration Manager (current branch) hierarchy where migration runs to import data from a source hierarchy.

Data gathering

The ongoing process of identifying the information in a source hierarchy that you can migrate to your destination hierarchy. Configuration Manager checks the source hierarchy on a schedule. This process identifies any changes to information in the source hierarchy that you previously migrated and that you might want to update in the

destination hierarchy.

For more information, see Data gathering.

Migration jobs

The process of configuring the specific objects to migrate, and then managing the migration of those objects to the destination hierarchy.

For more information, see Planning a migration job strategy.

Client migration

The process of transferring information that clients use from the database of the source site to the database of the destination hierarchy. This migration of data is then followed by an upgrade of client software on devices to the client software version from the destination hierarchy.

For more information, see Planning a client migration strategy.

Shared distribution points

The distribution points from the source hierarchy that Configuration Manager shares with the destination hierarchy during the migration period.

During the migration period, clients assigned to sites in the destination hierarchy can get content from shared distribution points.

For more information, see Share distribution points between source and destination hierarchies.

Monitoring migration

The process of monitoring migration activities. You monitor migration progress and success from the **Migration** node in the **Administration** workspace.

For more information, see Planning to monitor migration activity.

Stop gathering data

The process of stopping data gathering from source sites. When you no longer have data to migrate from a source hierarchy, or if you want to pause migration-related activities, you can configure the destination hierarchy to stop gathering data from the source hierarchy.

For more information, see Data gathering.

Clean up migration data

The process of finishing migration from a source hierarchy by removing information about the migration from the destination hierarchies database.

For more information, see Planning to complete migration.

Typical workflow

To set up a workflow for migration:

1. Specify a supported source hierarchy.
2. Set up data gathering. Data gathering enables Configuration Manager to collect information about data that can migrate from the source hierarchy.

   Configuration Manager automatically repeats the process to collect data on a simple schedule until you stop the data gathering process. By default, the data gathering process repeats every four hours so that Configuration Manager can identify changes to data in the source hierarchy. Data gathering is also necessary to share distribution points.
3. Create migration jobs to migrate data between the source and destination hierarchy.

4. You can stop the data gathering process at any time by using the **Stop Gathering Data** action. When you stop data gathering, Configuration Manager no longer identifies changes to data in the source hierarchy and can no longer share distribution points. Typically, you use this action when you no longer plan to migrate data or share distribution points from the source hierarchy.

5. Optionally, after data gathering has stopped at all sites for the source hierarchy, you can clean up the migration data by using the **Clean Up Migration Data** action. This action deletes the historical data about migration from a source hierarchy from the database of the destination hierarchy.

After you migrate data, and you no longer need the source hierarchy to manage devices in your environment, you can decommission that source hierarchy and infrastructure.

Scenarios

Configuration Manager supports the following migration scenarios:

- Migration from Configuration Manager 2007 hierarchies
- Migration from Configuration Manager 2012 or another Configuration Manager hierarchy

> **NOTE**
> The expansion of a hierarchy that has a standalone site into a hierarchy that has a central administration site isn't categorized as a migration. For information about hierarchy expansion, see Expand a stand-alone primary site.

Migration from Configuration Manager 2007 hierarchies

When you use migration to migrate data from Configuration Manager 2007, you can maintain your investment in your existing site infrastructure and gain the following benefits:

Site database improvements

The Configuration Manager (current branch) database supports full Unicode.

Database replication between sites

Replication in Configuration Manager (current branch) is based on Microsoft SQL Server. This behavior improves the performance of site-to-site data transfer.

User-centric management

Users are the focus of management tasks in Configuration Manager (current branch). For example, you can distribute software to a user even if you don't know the device name for that user. Additionally, Configuration Manager gives users much more control over what software is installed on their devices and when that software is installed.

Hierarchy simplification

Configuration Manager (current branch) lets you build a simpler site hierarchy. This improvement is due to the introduction of the central administration site type and changes to the behavior of primary and secondary sites. Configuration Manager (current branch) uses less network bandwidth and requires fewer servers than previous versions.

Role-based administration

This central security model in Configuration Manager (current branch) offers hierarchy-wide security and management that corresponds to your administrative and business requirements.

> **NOTE**
>
> Because of design changes that were first introduced in System Center 2012 Configuration Manager, you can't upgrade Configuration Manager 2007 to Configuration Manager (current branch). In-place upgrade is supported from System Center 2012 Configuration Manager to Configuration Manager (current branch).

Migration from Configuration Manager 2012 or another Configuration Manager hierarchy

The process of migrating data from a System Center 2012 Configuration Manager or Configuration Manager hierarchy is the same. This process includes migrating data from multiple source hierarchies into a single destination hierarchy. You might use this process when your company gets additional resources that are already managed by Configuration Manager. Additionally, you can migrate data from a test environment to your Configuration Manager production environment. This process lets you maintain your investment in the Configuration Manager test environment.

See also

- Planning for migration to Configuration Manager
- Configuring source hierarchies and source sites for migration
- Operations for migration
- Security and privacy for migration
- Start using Configuration Manager

Plan for migration to System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Before you migrate data to a System Center Configuration Manager destination hierarchy, make sure that you are familiar with sites and hierarchies in Configuration Manager. For more about sites and hierarchies, see Fundamentals of System Center Configuration Manager.

You must install a System Center Configuration Manager hierarchy to be the destination hierarchy before you migrate data from a supported source hierarchy.

After you install the destination hierarchy, set up the management features and functions that you want to use in your destination hierarchy before you start to migrate data.

Additionally, you might have to plan for overlap between the source hierarchy and your destination hierarchy. For example, you might set up the source hierarchy to use the same network locations or boundaries as your destination hierarchy, and you then install new clients to your destination hierarchy and use automatic site assignment. In this scenario, because a newly installed Configuration Manager client can select a site to join from either hierarchy, the client might incorrectly assign to your source hierarchy. Therefore, plan to assign each new client in the destination hierarchy to a specific site in that hierarchy instead of using automatic site assignment.

For more about site assignments, see Client site assignment considerations in Interoperability between different versions of System Center Configuration Manager.

Plan Topics

Use the following topics to help you plan how to migrate a supported source hierarchy to a System Center Configuration Manager destination hierarchy:

- Prerequisites for migration in System Center Configuration Manager
- Administrator checklists for migration planning in System Center Configuration Manager
- Determine whether to migrate data to System Center Configuration Manager
- Plan a source hierarchy strategy in System Center Configuration Manager
- Administrator checklists for migration planning in System Center Configuration Manager
- Plan a client migration strategy in System Center Configuration Manager
- Plan a content deployment migration strategy in System Center Configuration Manager
- Plan for the migration of Configuration Manager objects to System Center Configuration Manager
- Plan to monitor migration activity in System Center Configuration Manager
- Plan to complete migration in System Center Configuration Manager

Prerequisites for migration in System Center Configuration Manager

9/11/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To migrate from a supported source hierarchy, you must have access to each applicable Configuration Manager source site, and permissions within the System Center Configuration Manager destination site to configure and run migration operations.

Use the information in the following sections to help you understand the versions of Configuration Manager that are supported for migration, and the required configurations.

- Versions of Configuration Manager that are supported for migration
- Source site languages that are supported for migration
- Required configurations for migration

Versions of Configuration Manager that are supported for migration

You can migrate data from a source hierarchy that runs any of the following versions of Configuration Manager:

- Configuration Manager 2007 SP2 (For the purpose of migration, Configuration Manager 2007 R2 or R3 on the source site are not a consideration. So long as the source site runs SP2, sites with either the R2 or R3 add-on installed are supported for migration to System Center Configuration Manager).
- System Center 2012 Configuration Manager SP2 or System Center 2012 R2 Configuration Manager SP1.

  > **TIP**
  > In addition to migration, you can use an in-place upgrade of sites that run System Center 2012 Configuration Manager to System Center Configuration Manager.

- A System Center Configuration Manager hierarchy of the same or lesser version of System Center Configuration Manager.

  For example, if you have a destination hierarchy that runs System Center Configuration Manager 1606, you could use migration to copy data from a source hierarchy that runs version 1606 or 1602. However you could not migrate data from a source hierarchy that runs 1610.

Source site languages that are supported for migration

When you migrate data between Configuration Manager hierarchies, the data is stored in the destination hierarchy in the language neutral format for System Center Configuration Manager. Because Configuration Manager 2007 does not store data in a language neutral format, the migration process must convert objects to this format during migration from Configuration Manager 2007. Therefore, only Configuration Manager 2007 source sites that are installed with the following languages are supported for migration:

- English
- French

- German
- Japanese
- Korean
- Russian
- Simplified Chinese
- Traditional Chinese

When you migrate data from a System Center 2012 Configuration Manager or System Center Configuration Manager hierarchy, there are no source site language limitations. Objects in the source site database are already in a language neutral format.

Required configurations for migration

The following are required configurations for using migration and migration operations:

- **To configure, run, and monitor migration in the Configuration Manager console:**

  In the destination site, your account must be assigned the role-based administration security role of **Infrastructure Administrator**. This security role grants permissions to manage all migration operations, which includes the creation of migration jobs, clean up, monitoring, and the action to share and upgrade distribution points.

- **Data Gathering:**

  To enable the destination site to gather data, you must configure the following two source site access accounts for use with each source site:

  - **Source Site Account:** This account is used to access the SMS Provider of the source site.
    - For a Configuration Manager 2007 SP2 source site, this account requires **Read** permission to all source site objects.
    - For a System Center 2012 Configuration Manager or System Center Configuration Manager source site, this account requires **Read** permission to all source site objects, You grant this permission to the account by using role-based administration. For information about how to use role-based administration, see Fundamentals of role-based administration for System Center Configuration Manager.
  - **Source Site Database Account:** This account is used to access the SQL Server database of the source site and requires **Connect**, **Execute**, and **Select** permissions to the source site database.

  You can configure these accounts when you configure a new source hierarchy, data gathering for an additional source site, or when you reconfigure the credentials for a source site. These accounts can use a domain user account, or you can specify the computer account of the top-level site of the destination hierarchy.

  > **IMPORTANT**
  > If you use the Configuration Manager computer account for either access account, ensure that this account is a member of the security group **Distributed COM Users** in the domain where the source site resides.

  When gathering data, the following network protocols and ports are used:

  - NetBIOS/SMB - 445 (TCP)

- RPC (WMI) - 135 (TCP)
- SQL Server - The TCP ports in use by both the source and destination site databases.

- **Migrate Software Updates:**

  Before you migrate software updates, you must configure the destination hierarchy with a software update point. For more information, see Planning to migrate software updates.

- **Share distribution points:**

  To successfully share any distribution points from a source site, at least one primary site or the central administration site in the destination hierarchy must use the same port numbers for client requests as the source site. For information about client request ports, see How to configure client communication ports in System Center Configuration Manager

  For each source site, only the distribution points that are installed on site system servers that are configured with a FQDN are shared.

  In addition, to share a distribution point from a System Center 2012 Configuration Manager or System Center Configuration Manager source site, the **Source Site Account** (which accesses the SMS Provider for the source site server), must have **Modify** permissions to the **Site** object on the source site. You grant this permission to the account by using role-based administration. For information about how to use role-based administration, see Fundamentals of role-based administration for System Center Configuration Manager.

- **Upgrade or reassign distribution points:**

  The **Source Site Access Account** configured to gather data from the SMS Provider of the source site must have the following permissions:

  - To upgrade a Configuration Manager 2007 distribution point, the account requires **Read**, **Execute**, and **Delete** permissions to the **Site** class on the Configuration Manager2007 site server to successfully remove the distribution point from the Configuration Manager2007 source site
  - To reassign a System Center 2012 Configuration Manager or System Center Configuration Manager distribution point, the account must have **Modify** permission to the **Site** object on the source site. You grant this permission to the account by using role-based administration. For information about how to use role-based administration, see Fundamentals of role-based administration for System Center Configuration Manager.

    To successfully upgrade or reassign a distribution point to a new hierarchy, the ports that are configured for client requests at the site that manages the distribution point in the source hierarchy must match the ports that are configured for client requests at the destination site that will manage the distribution point. For information about client request ports, see How to configure client communication ports in System Center Configuration Manager.

Administrator checklists for migration planning in System Center Configuration Manager

2/12/2019 • 7 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the following administrator checklists to help you plan your migration strategy to System Center Configuration Manager.

Administrator checklist for migration planning

Use the following checklist for pre-migration planning steps.

- **Assess the current environment:**

  Identify existing business requirements that are met by the source hierarchy and develop plans to continue to meet those requirements in the destination hierarchy.

- **Review the functionality and changes that are available with the version of Configuration Manager that you use, and use this information to help you design your destination hierarchy:**

  For more information, see Fundamentals of System Center Configuration Manager and What's new in System Center Configuration Manager.

- **Determine the administrative security model to use for role-based administration:**

  For more information, see Fundamentals of role-based administration for System Center Configuration Manager.

- **Assess your network and Active Directory topology:** Review your existing domain structure and network topology and consider how this influences your hierarchy design and migration tasks.

- **Finalize your destination hierarchy design:**

  Decide upon the placement of a central administration site, primary sites, secondary sites, and content distribution options.

- **Map your hierarchy to the computers that you will use for sites and site servers in the destination hierarchy:**

  Identify the computers that sites and site system servers will use in the destination hierarchy, and then ensure that they have sufficient capacity to meet existing and future operational requirements.

- **Plan your object migration strategy:**

  Plan to use the available migration jobs to migrate different objects, including site boundaries, collections, advertisements, and deployments. For more information, see Types of migration jobs in Planning a migration job strategy in System Center Configuration Manager

  Configuration Manager migrates only the objects that you select. Any objects that are not migrated and that are required in the destination hierarchy must be re-created in the destination hierarchy.

  Objects that can migrate are displayed when you configure migration jobs.

- **Plan your client migration strategy:**

Plan to migrate clients by using a controlled approach that limits the network bandwidth and server processing requirements when you migrate clients to the destination hierarchy. For more about planning a client migration strategy, see Planning a client migration strategy in System Center Configuration Manager.

- **Plan for inventory and compliance data:**

  Configuration Manager does not support migrating hardware inventory, software inventory, or desired configuration management compliance data for software updates or clients.

  Instead, after the client migrates to its new site in the destination hierarchy and receives policy for these configurations, the client submits this information to its assigned site. This action populates the destination site database with current inventory and compliance data.

- **Plan for the completion of migration from the source hierarchy:**

  Decide when objects and clients will be migrated. After migration completes, you can plan to decommission the site servers in the source hierarchy.

Administrator checklist for hierarchy migration

Use the following checklist to help you plan a destination hierarchy before you start migration.

- **Identify the computers to use in the destination hierarchy:**

  Configuration Manager does not support an in-place upgrade from Configuration Manager 2007 infrastructure. Instead you use migration to move data from Configuration Manager 2007 to System Center Configuration Manager. This requires you to use a side-by-side deployment and install System Center Configuration Manager on new computers.

  Similarly, when you migrate from another System Center Configuration Manager hierarchy, you must install a new destination hierarchy that is a side-by-side deployment to your source hierarchy.

- **Create your destination hierarchy:**

  To prepare for migration, install and configure a System Center Configuration Manager destination hierarchy that includes a primary site. For example:

  - Install a central administration site and then install at least one child primary.
  - Install a stand-alone primary if you do not plan to use a central administration site.

- **If you want to migrate information that is related to software updates, configure a software update point in the destination hierarchy and synchronize software updates:**

  You must configure and synchronize software updates in the destination hierarchy before you can migrate software updates information from the source hierarchy.

- **Install and configure additional site system roles in the destination hierarchy:**

  Configure additional site system roles and site systems that you require.

- **Check operational functionality in the destination hierarchy:**

  Check the following:

  - If the destination hierarchy includes multiple sites, confirm that database replication is working between sites. Database replication is not applicable to stand-alone primary sites.
  - Check that all installed site system roles are operational.
  - Check that the Configuration Manager clients you install to the destination hierarchy can

communicate successfully with their assigned site.

Administrator checklist for migration

Use the following checklist to migrate data from the source hierarchy to the destination hierarchy.

- **Enable migration in the destination hierarchy:**

  Configure a source hierarchy by specifying the top-level site of the source hierarchy. For more about specifying the source site, see Planning a source hierarchy strategy in System Center Configuration Manager.

- **When the source hierarchy runs Configuration Manager 2007 SP2, select and configure additional sites in the source hierarchy:**

  For each additional site in the Configuration Manager 2007 SP2 source hierarchy that you want to collect data from, you must configure credentials for data gathering. When you configure each source site, the data-gathering process begins immediately and continues throughout the migration period until you stop data gathering for that site. Data gathering ensures that you can migrate objects from the source hierarchy that are updated or added after a previous data-gathering process.

  > **NOTE**
  > When the source hierarchy runs System Center 2012 Configuration Manager or later, you do not need to configure additional source sites.

- **Configure distribution point sharing:**

  You can share distribution points between the two hierarchies to make content for objects that you migrate available to clients in the destination hierarchy. This ensures that the same content remains available for clients in both hierarchies and that you can maintain this content until you stop gathering data and finish the migration.

  For information about shared distribution points, see Share distribution points between source and destination hierarchies in Planning a content deployment migration strategy in System Center Configuration Manager.

- **Create and run migration jobs to migrate objects associated with the clients in the source hierarchy:**

  Create migration jobs to migrate objects between hierarchies. The required configurations for each migration job can vary depending on what data the job migrates.

  For example, when you migrate content, regardless of the migration job you use, you must assign a site in the destination hierarchy to own management of that content. The assigned site will access the original source file location for the content and is responsible for distributing that content to distribution points in the destination hierarchy.

  For more information, see Create and edit migration jobs for system center configuration manager in Operations for migrating to System Center Configuration Manager.

- **Migrate clients to the destination hierarchy:**

  The process of migrating clients depends on your migration scenario:

  - When you migrate clients that have a client version that is not the same as the destination hierarchy, you must upgrade the client software. Upgrade requires the removal of the current Configuration Manager client, followed by the installation of the new client version that matches the destination

site.

- When you migrate clients that have a client version that matches the version of the destination hierarchy, the client does not upgrade or reinstall. Instead, the client reassigns to a primary site in the destination hierarchy.

When you migrate a client to the destination hierarchy, the client is associated with its data that you previously migrated to that destination hierarchy.

For more information, see Planning a client migration strategy in System Center Configuration Manager.

- **Upgrade or reassign shared distribution points:**

  When you no longer have to support clients in your source hierarchy, you can upgrade shared distribution points from a Configuration Manager 2007 source site, or reassign shared distribution points from a System Center 2012 Configuration Manager or System Center Configuration Manager source site. When you upgrade or reassign a distribution point, the site system role transfers to a primary site in the destination hierarchy and the distribution point is removed from the source site in the source hierarchy. When you upgrade or reassign a shared distribution point, the content remains on the distribution point computer and you do not have to redeploy the content to new distribution points in the destination hierarchy.

  You can also upgrade a distribution point that is co-located on a Configuration Manager 2007 secondary site server. This removes the secondary site and results in only a distribution point in the destination hierarchy.

  For information about shared distribution points, see Share distribution points between source and destination hierarchies in Planning a content deployment migration strategy in System Center Configuration Manager.

- **Finish migration:**

  After you have migrated data and clients from all sites in the source hierarchy and you have upgraded applicable distribution points, you can finish migration. To finish migration you stop gathering data for each source site in the source hierarchy. You can then remove migration information that you do not need and decommission your source hierarchy infrastructure. For more information, see Planning to complete migration in System Center Configuration Manager.

Determine whether to migrate data to System Center Configuration Manager

2/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

In System Center Configuration Manager, migration provides a process for transferring data and configurations that you've created from supported versions of Configuration Manager to your new hierarchy. You can use this to:

- Combine multiple hierarchies into one.
- Move data and configurations from a lab deployment into your production deployment.
- Move data and configuration from a prior version of Configuration Manager, like Configuration Manager 2007, which has no upgrade path to System Center Configuration Manager, or from System Center 2012 Configuration Manager (which does support an upgrade path to System Center Configuration Manager).

With the exception of the distribution point site system role and the computers that host distribution points, no infrastructure (which includes sites, site system roles, or computers that host a site system role), migrates, transfers, or can be shared between hierarchies.

Although you cannot migrate server infrastructure, you can migrate Configuration Manager clients between hierarchies. Client migration involves migrating the data that clients use from the source hierarchy to the destination hierarchy, and then installing or reassigning the client software so that the client then reports to the new hierarchy.

After you install a client to the new hierarchy and the client submits its data, its unique Configuration Manager ID helps Configuration Manager associate the data that you previously migrated with each client computer.

The functionality that's provided by migration helps you maintain investments that you have made in configurations and deployments while letting you take full advantage of core changes in the product first (which was first introduced in System Center 2012 Configuration Manager and then continued in System Center Configuration Manager). These changes include a simplified Configuration Manager hierarchy that uses fewer sites and resources, and the improved processing that comes from using native 64-bit code that runs on 64-bit hardware.

For information about the versions of Configuration Manager that migration supports, see Prerequisites for migration in System Center Configuration Manager.

The following sections help you plan for data that you can or can't migrate:

- Data that you can migrate to System Center Configuration Manager
- Data that you can't migrate to System Center Configuration Manager

Data that you can migrate to System Center Configuration Manager

Migration can migrate most objects between supported Configuration Manager hierarchies. The migrated instances of some objects from a supported version of Configuration Manager 2007 must be modified to conform to the System Center 2012 Configuration Manager schema and object format.

These modifications don't affect the data in the source site database. Objects that are migrated from a supported version of System Center 2012 Configuration Manager or System Center Configuration Manager do not require

modification.

The following are objects that can migrate based on the version of Configuration Manager in the source hierarchy. Some objects, like queries, do not migrate. If you want to continue to use these objects that do not migrate you must recreate them in the new hierarchy. Other objects, including some client data, are automatically recreated in the new hierarchy when you manage clients in that hierarchy.

Objects that you can migrate from System Center 2012 Configuration Manager or System Center Configuration Manager current branch

- Applications for System Center 2012 Configuration Manager and later versions
- App-V Virtual Environment from System Center 2012 Configuration Manager and later versions
- Asset Intelligence customizations
- Boundaries
- Collections: To migrate collections from a supported version of System Center 2012 Configuration Manager or System Center Configuration Manager, you use an object migration job.
- Compliance settings:
  - Configuration baselines
  - Configuration items
- Deployments
- Operating system deployment:
  - Boot images
  - Driver packages
  - Drivers
  - Images
  - Packages
  - Task sequences
- Search results: Saved search criteria
- Software updates:
  - Deployments
  - Deployment packages
  - Templates
  - Software update lists
- Software distribution packages
- Software metering rules
- Virtual application packages

Objects that you can migrate from Configuration Manager 2007 SP2

- Advertisements
- Applications for System Center 2012 Configuration Manager and later versions

- App-V Virtual Environment from System Center 2012 Configuration Manager and later versions
- Asset Intelligence customizations
- Boundaries
- Collections: You migrate collections from a supported version of Configuration Manager 2007 by using a collection migration job.
- Compliance settings (referred to as desired configuration management in Configuration Manager 2007):
  - Configuration baselines
  - Configuration items
- Operating system deployment:
  - Boot images
  - Driver packages
  - Drivers
  - Images
  - Packages
  - Task sequences
- Search results: Search folders
- Software updates:
  - Deployments
  - Deployment packages
  - Templates
  - Software update lists
- Software distribution packages
- Software metering rules
- Virtual application packages

Data that you cannot migrate to System Center Configuration Manager

You cannot migrate the following types of objects:

- AMT client provisioning information
- Files on clients, including:
  - Client inventory and history data
  - Files in the client cache
- Queries
- Configuration Manager 2007 security rights and instances for the site and objects
- Configuration Manager 2007 reports from SQL Server Reporting Services

- Configuration Manager 2007 web reports
- System Center 2012 Configuration Manager and System Center Configuration Manager reports
- System Center 2012 Configuration Manager and System Center Configuration Manager role-based administration:
    - Security roles
    - Security scopes

Plan a source hierarchy strategy in System Center Configuration Manager

9/11/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Before you set up a migration job in your System Center Configuration Manager environment, you must configure a source hierarchy and gather data from at least one source site in that hierarchy. Use the following sections to help you plan for configuring source hierarchies, configuring source sites, and determining how Configuration Manager gathers information from the source sites in the source hierarchy.

Source hierarchies

A source hierarchy is a Configuration Manager hierarchy that has data that you want to migrate. When you set up migration and specify a source hierarchy, you specify the top-level site of the source hierarchy. This site is also called a source site. Additional sites that you can migrate data from in the source hierarchy are also called source sites.

- When you set up a migration job to migrate data from a Configuration Manager 2007 source hierarchy, you configure it to migrate data from one or more specific source sites in the source hierarchy.
- When you set up a migration job to migrate data from a source hierarchy that runs System Center 2012 Configuration Manager or later, you only need to specify the top-level site.

You can set up only one source hierarchy at a time.

- If you set up a new source hierarchy, that hierarchy automatically becomes the current source hierarchy replacing the previous source hierarchy.
- When you set up a source hierarchy, you must specify the top-level site of the source hierarchy and specify credentials for Configuration Manager to use to connect to the SMS Provider and site database of that source site.
- Configuration Manager uses these credentials to run data gathering to retrieve information about the objects and distribution points from the source site.
- As part of the data gathering process, child sites in the source hierarchy are identified.
- If the source hierarchy is a Configuration Manager 2007 hierarchy, you can set up those additional sites as source sites with separate credentials for each source site.

Although you can set up multiple source hierarchies in succession, migration is active for only one source hierarchy at a time.

- If you set up an additional source hierarchy before you complete migration from the current source hierarchy, Configuration Manager cancels any active migration jobs and postpones any scheduled migration jobs for the current source hierarchy.
- The newly configured source hierarchy then becomes the current source hierarchy, and the original source hierarchy is now inactive.
- You can then set up connection credentials, additional source sites, and migration jobs for the new source hierarchy.

If you restore an inactive source hierarchy and have not previously used **Cleanup Migration Data**, you can view the previously configured migration jobs for that source hierarchy. However, before you can continue migration from that hierarchy, you must reconfigure the credentials to connect to applicable source sites in the hierarchy, and then reschedule any migration jobs that did not finish.

Caution

If you migrate data from more than a single source hierarchy, each additional source hierarchy must contain a unique set of site codes.
Source and destination hierarchies also requires different set of site codes.

For more about configuring a source hierarchy, see Configuring source hierarchies and source sites for migration to System Center Configuration Manager

Source sites

Source sites are the sites in the source hierarchy that have the data that you want to migrate. The top-level site of the source hierarchy is always the first source site. When migration collects data from the first source site of a new source hierarchy, it discovers information about additional sites in that hierarchy.

After data gathering completes for the initial source site, the actions you take next depend on the product version of the source hierarchy.

Source sites that run Configuration Manager 2007 SP2

After data is gathered from the initial source site of the Configuration Manager 2007 SP2 hierarchy, you do not have to set up additional source sites before you create migration jobs. However, before you can migrate data from additional sites, you must set up additional sites as source sites, and System Center Configuration Manager must successfully gather data from those sites.

To gather data from additional sites, you individually set up each site as a source site. This requires you to specify the credentials for System Center Configuration Manager to connect to the SMS Provider and site database of each source site. After you set up the credentials for a source site, the data gathering process for that site begins.

When you set up additional source sites in a Configuration Manager 2007 SP2 source hierarchy, you must set up source sites from the top down, which means you set up the bottom-tier sites last. You can configure source sites in a branch of the hierarchy at any time, but you must set up a site as a source site before you set up any of its child sites as source sites.

> **NOTE**
> Only primary sites in a Configuration Manager 2007 SP2 hierarchy are supported for migration.

Source sites that run System Center 2012 Configuration Manager or later

After data is gathered from the initial source site of the System Center 2012 Configuration Manager or later hierarchy, you do not have to set up additional source sites in that source hierarchy. This is because unlike Configuration Manager 2007, these versions of Configuration Manager use a shared database, and the shared database lets you identify and then migrate all available objects from the initial source site.

When you set up the access accounts to gather data, you might need to grant the **Source Site SMS Provider Account** access to multiple computers in the source hierarchy. This might be needed when the source site supports multiple instances of the SMS Provider, each on a different computer. When data gathering begins, the top-level site of the destination hierarchy contacts the top-level site in the source hierarchy to identify the locations of the SMS Provider for that site. Only the first instance of the SMS provider is identified. If the data gathering process cannot access the SMS Provider at the location it identifies, the process fails and does not try to connect to additional computers that run an instance of SMS Provider for that site.

Data gathering

Immediately after you specify a source hierarchy, set up credentials for each additional source site in a source hierarchy, or share the distribution points for a source site, Configuration Manager starts to gather data from the source site.

The data gathering process then repeats itself on a simple schedule to maintain synchronization with any changes to data in the source site. By default, the process repeats every four hours. You can change the schedule for this cycle by editing the **Properties** of the source site. The initial data gathering process must review all objects in the Configuration Manager database and can take a long time to finish. Subsequent data gathering processes identify only changes to the data and require less time to finish.

To gather data, the top-level site in the destination hierarchy connects to the SMS Provider and the site database of the source site to retrieve a list of objects and distribution points. These connections use the source site access accounts. For information about required configurations for gathering data, see Prerequisites for migration in System Center Configuration Manager.

You can start and stop the data gathering process by using **Gather Data Now** and **Stop Gathering Data** in the Configuration Manager console.

After you use **Stop Gathering Data** for a source site for any reason, you must reconfigure credentials for the site before you can gather data from that site again. Until you reconfigure the source site, Configuration Manager cannot identify new objects or changes to previously migrated objects at that site.

> **NOTE**
> Before you expand a standalone primary site into a hierarchy with a central administration site, you must stop all data gathering. You can reconfigure data gathering after the site expansion completes.

Gather Data Now

After the initial data gathering process runs for a site, this process repeats itself to identify objects that have updated since the last data gathering cycle. You can also use the **Gather Data Now** action in the Configuration Manager console to immediately start the process and to reset the start time of the next cycle.

After a data gathering process successfully finishes for a source site, you can share the distribution points from the source site and configure migration jobs to migrate data from the site. Data gathering is a repeating process for migration, and it continues until you change the source hierarchy or use **Stop Gathering Data** to end the data gathering process for that site.

Stop Gathering Data

You can use **Stop Gathering Data** to end the data gathering process for a source site when you no longer want Configuration Manager to identify new or changed objects from that site. This action also prevents Configuration Manager from offering clients in the destination hierarchy any shared distribution points from the source as content locations for the content that you have migrated.

To stop gathering data from each source site, you must run **Stop Gathering Data** on the bottom-tier source sites, and then repeat the process at each parent site. The top-level site of the source hierarchy must be the last site on which you stop gathering data. You must stop data gathering at each child site before performing this action at a parent site. Typically, you only stop gathering data when you are ready to complete the migration process.

After you stop gathering data for a source site, information previously gathered about objects and collections from that site remain available to use when you set up new migration jobs. However, you do not see any new objects or collections, nor do you see changes that were made to existing objects. If you reconfigure the source site and begin gathering data again, you will see information and status about previously migrated objects.

Plan a migration job strategy in System Center Configuration Manager

7/9/2019 • 15 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use migration jobs to configure the specific data that you want to migrate to your System Center Configuration Manager environment. Migration jobs identify the objects that you plan to migrate, and they run at the top-level site in your destination hierarchy. You can set up one or more migration jobs per source site. This lets you migrate all objects at one time or limited subsets of data with each job.

You can create migration jobs after Configuration Manager has successfully gathered data from one or more sites from the source hierarchy. You can migrate data in any sequence from the source sites that have gathered data. With a Configuration Manager 2007 source site, you can migrate data only from the site where an object was created. With source sites that run System Center 2012 Configuration Manager or later, all data that you can migrate is available at the top-level site of the source hierarchy.

Before you migrate clients between hierarchies, ensure that the objects that clients use have migrated and that these objects are available in the destination hierarchy. For example, when you migrate from a Configuration Manager 2007 SP2 source hierarchy, you might have an advertisement for content that is deployed to a custom collection that has a client. In this scenario, we recommend that you migrate the collection, the advertisement, and the associated content before you migrate the client. This data cannot be associated with the client in the destination hierarchy if the content, collection, and advertisement are not migrated before the client migrates. If a client is not associated with the data related to a previously run advertisement and content, the client can be offered the content for installation in the destination hierarchy, which might be unnecessary. When the client migrates after the data has migrated, the client is associated with this content and advertisement, and unless the advertisement is recurring, is not offered this content for the migrated advertisement again.

Some objects require more than the migration of data from the source hierarchy to the destination hierarchy. For example, to successfully migrate software updates for your clients to your destination hierarchy, you must deploy an active software update point, configure the catalog of products, and synchronize the software update point with Windows Server Update Services (WSUS) in the destination hierarchy.

Types of migration jobs

Configuration Manager supports the following types of migration jobs. Each job type is designed to help define the objects that you can include in that job.

Collection migration (only supported when migrating from Configuration Manager 2007 SP2): Migrate objects that are related to collections you select. By default, collection migration includes all objects that are associated with members of the collection. You can exclude specific object instances when you use a collection migration job.

Object migration: Migrate individual objects that you select. You select only the specific data that you want to migrate.

Previously migrated object migration: Migrate objects that you previously migrated when they have updated in the source hierarchy after they were last migrated.

Objects that you can migrate

Not every object can migrate by a specific type of migration job. The following list identifies the type of objects that you can migrate with each type of migration job.

> **NOTE**
> Collection migration jobs are available only when you migrate objects from a Configuration Manager 2007 SP2 source hierarchy.

Job types you can use to migrate each object

- **Advertisements** (available to migrate from supported Configuration Manager 2007 source sites)
  - Collection migration
- **Asset Intelligence catalog**
  - Object migration
  - Previously migrated object migration
- **Asset Intelligence hardware requirements**
  - Object migration
  - Previously migrated object migration
- **Asset Intelligence software list**
  - Object migration
  - Previously migrated object migration
- **Boundaries**
  - Object migration
  - Previously migrated object migration
- **Configuration baselines**
  - Collection migration
  - Object migration
  - Previously migrated object migration
- **Configuration items**
  - Collection migration
  - Object migration
  - Previously migrated object migration
- **Maintenance windows**
  - Collection migration
- **Operating system deployment boot images**
  - Collection migration
  - Object migration
  - Previously migrated object migration
- **Operating system deployment driver packages**

- Collection migration
- Object migration
- Previously migrated object migration

- **Operating system deployment drivers**
  - Collection migration
  - Object migration
  - Previously migrated object migration
- **Operating system deployment images**
  - Collection migration
  - Object migration
  - Previously migrated object migration
- **Operating system deployment packages**
  - Collection migration
  - Object migration
  - Previously migrated object migration
- **Software distribution packages**
  - Collection migration
  - Object migration
  - Previously migrated object migration
- **Software metering rules**
  - Object migration
  - Previously migrated object migration
- **Software update deployment packages**
  - Collection migration
  - Object migration
  - Previously migrated object migration
- **Software update deployment templates**
  - Collection migration
  - Object migration
  - Previously migrated object migration
- **Software update deployments**
  - Collection migration
- **Software update lists**
  - Object migration

- Previously migrated object migration

- **Task sequences**
  - Collection migration
  - Object migration
  - Previously migrated object migration
- **Virtual application packages**
  - Collection migration
  - Object migration

> **IMPORTANT**
>
> Although you can migrate a virtual application package by using object migration, the packages cannot be migrated by using the migration job type of **Previously Migrated Object Migration**. Instead, you must delete the migrated virtual application package from the destination site and then create a new migration job to migrate the virtual application.

General planning for all migration jobs

Use the Create Migration Job wizard to create a migration job to migrate objects to your destination hierarchy. The type of the migration job that you create determines which objects are available to migrate. You can create and use multiple migration jobs to migrate data from the same source site or from multiple source sites. The use of one type of migration job does not block the use of a different type of migration job.

After a migration job runs successfully, its status is listed as **Completed** and it cannot be run again. However, you can create a new migration job to migrate any of the objects that were migrated by the original job, and the new migration job can include additional objects as well. When you create additional migration jobs, the objects that have been previously migrated show the state of **Migrated**. You can select these objects to migrate them again, but unless the object has been updated in the source hierarchy, migrating these objects again is not necessary. If the object has been updated in the source hierarchy after it was originally migrated, you can identify that object when you use the migration job type of **Objects modified after migration**.

You can delete a migration job before it runs. However, after a migration job finishes, it remains visible in the Configuration Manager console and cannot be deleted. Each migration job that has finished or has not yet run remains visible in the Configuration Manager console until you finish the migration process and clean up migration data.

> **NOTE**
>
> After you have finished migration by using the **Clean Up Migration Data** action, you can reconfigure the same hierarchy as the current source hierarchy to restore visibility to the objects you previously migrated.

You can view the objects contained in any migration job in the Configuration Manager console by selecting the migration job and then choosing the **Objects in Job** tab.

Use the information in the following sections to help you plan for all migration jobs.

Data selection

When you create a collection migration job, you must select one or more collections. After you select the collections, the Create Migration Job wizard shows the objects that are associated with the collections. By default,

all objects associated with the selected collections are migrated, but you can uncheck the objects that you do not want to migrate with that job. When you uncheck an object that has dependent objects, those dependent objects are also unchecked. All unchecked objects are added to an exclusion list. Objects on an exclusion list are removed from automatic selection for future migration jobs. You must manually edit the exclusion list to remove objects that you want to have automatically selected for migration in migration jobs you create in the future.

Site ownership for migrated content

When you migrate content for deployments, you must assign the content object to a site in the destination hierarchy. This site then becomes the owner for that content in the destination hierarchy. Although the top-level site of your destination hierarchy is the site that actually migrates the metadata for content, it is the assigned site that accesses the original source files for the content across the network.

To minimize the network bandwidth that is used during migration, consider transferring ownership of content to the closest available site. Because information about the content is shared globally in System Center Configuration Manager, it will be available at every site.

Information about content is shared to all sites in the destination hierarchy by using database replication. However, any content that you assign to a primary site and then deploy to distribution points at other primary sites transfers by using file-based replication. This transfer is routed through the central administration site and then to each additional primary site. By centralizing packages that you plan to distribute to multiple primary sites before or during migration when you assign a site as the content owner, you can reduce data transfers across low-bandwidth networks.

Role-based administration security scopes for migrated data

When you migrate data to a destination hierarchy, you must assign one or more role-based administration security scopes to the objects whose data is migrated. This ensures that only the appropriate administrative users have access to this data after it is migrated. The security scopes that you specify are defined by the migration job and are applied to each object that is migrated by that job. If you require different security scopes to be applied to different sets of objects and you want to assign those scopes during migration, you must migrate the different sets of objects by using different migration jobs.

Before you set up a migration job, review how role-based administration works in System Center Configuration Manager. If necessary, set up one or more security scopes for the data that you migrate to control who will have access to the migrated objects in the destination hierarchy.

For more about security scopes and role-based administration, see Fundamentals of role-based administration for System Center Configuration Manager.

Review migration actions

When you set up a migration job, the Create Migration Job wizard shows a list of actions that you must take to ensure a successful migration and a list of actions that Configuration Manager takes during the migration of the selected data. Review this information carefully to check the expected outcome.

Schedule migration jobs

By default, a migration job runs immediately after it is created. However, you can specify when the migration job runs when you create the job or by editing the properties of the job. You can schedule the migration job to run as follows:

- Run the job now
- Run the job at a specific start time
- Not run the job

Specify conflict resolution for migrated data

By default, migration jobs do not overwrite data in the destination database unless you configure the migration job

to skip or overwrite data that has previously been migrated to the destination database.

Plan for collection migration jobs

Collection migration jobs are available only when you migrate data from a source hierarchy that runs a supported version of Configuration Manager 2007. You must specify one or more collections to migrate when you migrate by collection. For each collection that you specify, the migration job automatically selects all related objects for migration. For example, if you select a specific collection of users, the collection members are then identified, and you can migrate the deployments associated with that collection. Optionally, you can select other deployment objects to migrate that are associated with those members. All these selected items are added to the list of objects that can be migrated.

When you migrate a collection, System Center Configuration Manager also migrates collection settings, including maintenance windows and collection variables, but it cannot migrate collection settings for AMT client provisioning.

Use the information in the following sections to learn about additional configurations that can apply to collection-based migration jobs.

Exclude objects from collection migration jobs

You can exclude specific objects from a collection migration job. When you exclude a specific object from a collection migration job, that object is added to a global exclusion list that has all the objects that you have excluded from migration jobs created for any source site in the current source hierarchy. Objects on the exclusion list are still available for migration in future jobs but are not automatically included when you create a new collection-based migration job.

You can edit the exclusion list to remove objects that you have previously excluded. After you remove an object from the exclusion list, it is then automatically selected when an associated collection is specified during the creation of a new migration job.

Unsupported collections

Configuration Manager can migrate any of the default user collections, device collections, and most custom collections from a Configuration Manager 2007 source hierarchy. However, Configuration Manager cannot migrate collections that contain users and devices in the same collection.

The following collections cannot be migrated:

- A collection that has users and devices.
- A collection that has a reference to a collection of a different resource type. For example, a device-based collection that has either a subcollection or a link to a user-based collection. In this example, only the top-level collection migrates.
- A collection that has a rule to include unknown computers. The collection migrates, but the rule to include unknown computers does not migrate.

Empty collections

An empty collection is a collection that has no resources associated with it. When Configuration Manager migrates an empty collection, it converts the collection to an organizational folder that has no users or devices. This folder is created with the name of the empty collection under the **User Collections** or **Device Collections** node in the **Assets and Compliance** workspace in the Configuration Manager console.

Linked collections and subcollections

When you migrate collections that are linked to other collections or that have subcollections, Configuration Manager creates a folder under the **User Collections** or **Device Collections** node in addition to the linked collections and subcollections.

Collection dependencies and include objects

When you specify a collection to migrate in the Create Migration Job wizard, any dependent collections are automatically selected to be included with the job. This behavior ensures that all necessary resources are available after migration.

For example: You select a collection for devices that run Windows 7 and is named **Win_7**. This collection is limited to a collection that has all your client operating systems and is named **All_Clients**. The collection **All_Clients** will be automatically selected for migration.

Collection limiting

With System Center Configuration Manager, collections are global data and are evaluated at each site in the hierarchy. Therefore, plan how to limit the scope of a collection after it is migrated. During migration, you can identify a collection from the destination hierarchy to use to limit the scope of the collection that you are migrating so that the migrated collection does not include unanticipated members.

For example, in Configuration Manager 2007, collections are evaluated at the site that creates them and at child sites. An advertisement might be deployed to only a child site, and this would limit the scope for that advertisement to that child site. In comparison, with System Center Configuration Manager, collections are evaluated at each site and associated advertisements are then evaluated for each site. Collection limiting lets you refine the collection members based on another collection to avoid the addition of unexpected collection members.

Site code replacement

When you migrate a collection that has criteria that identifies a Configuration Manager 2007 site, you must specify a specific site in the destination hierarchy. This ensures that the migrated collection remains functional in your destination hierarchy and does not increase in scope.

Specify behavior for migrated advertisements

By default, collection-based migration jobs disable advertisements that migrate to the destination hierarchy. This includes any programs that are associated with the advertisement. When you create a collection-based migration job that has advertisements, you see the **Enable programs for deployment in Configuration Manager after an advertisement is migrated** option on the **Settings** page of the Create Migration Job wizard. If you select this option, programs that are associated with the advertisements are enabled after they have migrated. As a best practice, do not select this option. Instead, enable the programs after they have migrated when you can verify the clients that will receive them.

> **NOTE**
>
> You see the **Enable programs for deployment in Configuration Manager after an advertisement is migrated** option only when you are creating a collection-based migration job and the migration job contains advertisements.

To enable a program after migration, clear **Disable this program on computers where it is advertised** on the **Advanced** tab of the program properties.

Plan for object migration jobs

Unlike collection migration, you must select each object and object instance that you want to migrate. You can select the individual objects (like advertisements from a Configuration Manager 2007 hierarchy or a publication from a System Center 2012 Configuration Manager or System Center Configuration Manager hierarchy) to add to the list of objects to migrate for a specific migration job. Any objects that you do not add to the migration list are not migrated to the destination site by the object migration job.

Object-based migration jobs do not have any additional configurations to plan for beyond those applicable to all migration jobs.

Plan for previously migrated object migration jobs

When an object that you have already migrated to the destination hierarchy is updated in the source hierarchy, you can migrate that object again by using the **Objects modified after migration** job type. For example, when you rename or update the source files for a package in the source hierarchy, the package version increments in the source hierarchy. After the package version increments, the package can be identified for migration by this job type.

This job type is similar to the object migration type except that when you select objects to migrate, you can only select from objects that have been updated after they were migrated by a previous migration job.

When you select this job type, the conflict resolution behavior on the **Settings** page of the Create Migration Job wizard is configured to overwrite previously migrated objects. This setting cannot be changed.

> **NOTE**
>
> This migration job can identify objects that are automatically updated by the source hierarchy and objects that an administrative user updates.

Plan a client migration strategy in System Center Configuration Manager

2/12/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To migrate clients from the source hierarchy to a System Center Configuration Manager destination hierarchy, you must do two tasks. You must migrate the objects that are associated with the client and you must then reinstall or reassign the clients from the source hierarchy to the destination hierarchy. You migrate the objects first so that they are available when the clients are migrated. The objects associated with the client are migrated by using migration jobs. For information about how to migrate the objects that are associated with the client, see Planning a migration job strategy in System Center Configuration Manager.

Use the following sections to help you plan to migrate clients to the destination hierarchy.

- Plan to migrate clients to the destination hierarchy
- Plan to handle data maintained on clients during migration
- Plan for inventory and compliance data during migration

Plan to migrate clients to the destination hierarchy

When you migrate clients from a source hierarchy, the client software on the client computer upgrades to match the product version of the destination hierarchy.

- **A Configuration Manager 2007 source hierarchy:** When you migrate clients from a source hierarchy that runs a supported version of Configuration Manager, the client software upgrades to the client version for the destination hierarchy.
- **A System Center 2012 Configuration Manager or later source hierarchy:** When you migrate clients between hierarchies that are of the same product version, the client software does not change or upgrade. Instead, the client reassigns from the source hierarchy to a site in the destination hierarchy.

> **NOTE**
> When the product version of a hierarchy is not supported for migration to your destination hierarchy, upgrade all sites and clients in the source hierarchy to a compatible product version. After the source hierarchy upgrades to a supported product version, you can migrate between the hierarchies. For more information, see Versions of Configuration Manager that are supported for migration in Prerequisites for migration in System Center Configuration Manager.

Use the following information to help you plan the client migration:

- To upgrade or reassign clients from a source site to a destination site, you can use any client deployment method that is supported for deploying clients in the destination hierarchy. Typical client deployment methods include client push installation, software distribution, Group Policy, and software update-based client installation. For more information, see Client installation methods in System Center Configuration Manager.
- Ensure that the device that runs the client software in the source hierarchy meets the minimum hardware requirements and runs an operating system that is supported by the version of Configuration Manager in

the destination hierarchy.

- Before you migrate a client, run a migration job to migrate the information that the client will use in the destination hierarchy.
- Clients that upgrade retain their run history for deployments. This prevents deployments from rerunning unnecessarily in the destination hierarchy.
    - For Configuration Manager 2007 clients, advertisement run history is retained.
    - For clients from System Center 2012 Configuration Manager or System Center Configuration Manager, deployment run history is retained.
- You can migrate clients from sites in the source hierarchy in any order that you choose. However, consider migrating limited numbers of clients in phases rather than migrating large numbers of clients at a single time. A phased migration reduces the network bandwidth requirements and server processing when each newly upgraded client submits its initial full inventory and compliance data to its assigned site.
- When you migrate Configuration Manager 2007 clients, the existing client software is uninstalled from the client computer and the new client software is installed.
- Configuration Manager cannot migrate a Configuration Manager 2007 client that has the App-V client installed unless the App-V client version is 4.6 SP1 or later.

You can monitor the client migration process in the **Migration** node of the **Administration** workspace in the Configuration Manager console.

After you migrate the client to the destination hierarchy, you can no longer manage that device by using your source hierarchy, and you should consider removing the client from the source hierarchy. Although this is not a requirement when you migrate hierarchies, it can help prevent identification of a migrated client in a source hierarchy report, or an incorrect count of resources between the two hierarchies during the migration. For example, when a migrated client remains in the source site database, you might run a software updates report that incorrectly identifies the computer as an unmanaged resource when it is now managed by the destination hierarchy.

Plan to handle data maintained on clients during migration

When you migrate a client from its source hierarchy to the destination hierarchy, some information is retained on the device, while other information is not available on the device after migration.

The following information is retained on the client device:

- The unique identifier (GUID), which associates a client with its information in the Configuration Manager database.
- The advertisement or deployment history, which prevents clients from unnecessarily rerunning advertisements or deployments in the destination hierarchy.

The following information is not retained on the client device:

- The files in the client cache. If the client requires these files to install software, the client downloads them again from the destination hierarchy.
- Information from the source hierarchy about any advertisements or deployments that have not yet run. If you want the client to run the advertisements or deployments after it migrates, you must redeploy them to the client in the destination hierarchy.
- Information about inventory. The client resends this information to its assigned site in the destination hierarchy after the client migrates and the new client data has been generated.

- Compliance data. The client resends this information to its assigned site in the destination hierarchy after the client migrates and the new client data has been generated.

When a client migrates, information that is stored in the Configuration Manager client registry and file path is not retained. After migration, reapply these settings. Typical settings include the following:

- Power schemes
- Logging settings
- Local policy settings

Additionally, you might have to reinstall some applications.

Plan for inventory and compliance data during migration

Client inventory and compliance data is not saved when you migrate a client to the destination hierarchy. Instead, this information is recreated in the destination hierarchy when a client first sends its information to its assigned site. To help reduce the resulting network bandwidth requirements and server processing, consider migrating a small number of clients in phases rather than migrating a large number of clients at a single time.

Additionally, you cannot migrate customizations for hardware inventory from a source hierarchy. You must introduce these to the destination hierarchy independently from migration. For information about how to extend hardware inventory, see How to configure hardware inventory in System Center Configuration Manager.

Plan a content deployment migration strategy in System Center Configuration Manager

2/12/2019 • 22 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

While you actively migrate data to a System Center Configuration Manager destination hierarchy, Configuration Manager clients in both the source and destination hierarchies can maintain access to content that you deployed in the source hierarchy. You can also use migration to upgrade or reassign distribution points from the source hierarchy to become distribution points in the destination hierarchy. When you share and upgrade or reassign distribution points, this strategy can help you avoid having to redeploy content to new servers in the destination hierarchy for the clients that you migrate.

Although you can recreate and distribute content in the destination hierarchy, you can also use the following options to manage this content:

- Share distribution points in the source hierarchy with clients in the destination hierarchy.
- Upgrade standalone Configuration Manager 2007 distribution points or Configuration Manager 2007 secondary sites in the source hierarchy to become distribution points in the destination hierarchy.
- Reassign distribution points from a System Center Configuration Manager source hierarchy to a site in the destination hierarchy.

Use the following sections to help you plan for content deployment during migration:

Share distribution points between source and destination hierarchies

During migration, you can share distribution points from a source hierarchy with the destination hierarchy. You can use shared distribution points to make content that you have migrated from a source hierarchy immediately available to clients in the destination hierarchy without having to recreate that content, and then distribute it to new distribution points in the destination hierarchy. When clients in the destination hierarchy request content that is deployed to distribution points that you have shared, the shared distribution points can be offered to the clients as valid content locations.

In addition to being a valid content location for clients in the destination hierarchy while migration from the source hierarchy remains active, it is possible to upgrade or reassign a distribution point to the destination hierarchy. You can upgrade Configuration Manager 2007 shared distribution points and reassign System Center 2012 Configuration Manager shared distribution points. When you upgrade or reassign a shared distribution point, the distribution point is removed from the source hierarchy and becomes a distribution point in the

destination hierarchy. After you upgrade or reassign a shared distribution point, you can continue to use the distribution point in the destination hierarchy after migration from the source hierarchy is finished. For more about how to upgrade a shared distribution point, see Plan to upgrade Configuration Manager 2007 shared distribution points. For more about how to reassign a shared distribution point, see Plan to Reassign System Center Configuration Manager Distribution Points.

You can choose to share distribution points from any source site in your source hierarchy. When you share distribution points for a source site, child secondary sites are shared at each qualifying distribution point at that primary site and at each of the primary sites. To qualify to be a shared distribution point, the site system server that hosts the distribution point must be set up with a fully qualified domain name (FQDN). Any distribution points that are set up with a NetBIOS name are disregarded.

> **TIP**
> Configuration Manager 2007 does not require you to set up an FQDN for site system servers.

Use the following information to help you plan for shared distribution points:

- Distribution points that you share must meet the prerequisites for shared distribution points. For more about these prerequisites, see Required configurations for migration in Prerequisites for migration in System Center Configuration Manager.
- The share distribution point action is a site-wide setting that shares all qualifying distribution points at a source site and at any direct child secondary sites. You cannot select individual distribution points to share when you enable distribution point sharing.
- Clients in the destination hierarchy can receive content location information for packages that are distributed to distribution points that are shared from the source hierarchy. For distribution points from a Configuration Manager 2007 source hierarchy, this includes branch distribution points, distribution points on server shares, and standard distribution points.

  > **WARNING**
  > If you change the source hierarchy, shared distribution points from the original source hierarchy are no longer available and cannot be offered as content locations to clients in the destination hierarchy. If you reconfigure migration to use the original source hierarchy, the previously shared distribution points are restored as valid content location servers.

- When you migrate a package that is hosted on a shared distribution point, the package version must remain the same in the source and destination hierarchies. When a package version is not the same in the source and destination hierarchy, clients in the destination hierarchy cannot retrieve that content from the shared distribution point. Therefore, if you update a package in the source hierarchy, you must re-migrate the package data before clients in the destination hierarchy can retrieve that content from a shared distribution point.

  > **NOTE**
  > When you view details for a package that is hosted on a shared distribution point, the number of packages that display as **Hosted Migrated Packages** on the source site's **Shared Distribution Points** tab is not updated until the next data gathering cycle is finished.

- You can view shared distribution points and their properties in the **Source Hierarchy** node of the **Administration** workspace in the Configuration Manager console that connects to the destination hierarchy.

- You cannot use a shared distribution point from a Configuration Manager 2007 source hierarchy to host packages for Microsoft Application Virtualization (App-V). App-V packages must migrate and be converted for use by clients in the destination hierarchy. However, you can use a shared distribution point from a System Center 2012 Configuration Manager or System Center Configuration Manager source hierarchy to host App-V packages for clients in a destination hierarchy.
- When you share a protected distribution point from a Configuration Manager 2007 source hierarchy, the destination hierarchy creates a boundary group that includes the protected network locations of that distribution point. You cannot change this boundary group in the destination hierarchy. However, if you change the protected boundary information for the distribution point in the Configuration Manager 2007 source hierarchy, that change is reflected in the destination hierarchy after the next data gathering cycle finishes.

  > **NOTE**
  > System Center 2012 Configuration Manager and System Center Configuration Manager sites use the concept of preferred distribution points instead of protected distribution points. This condition only applies to distribution points that are shared from Configuration Manager 2007 source sites.

The eligible distribution points are not visible in the Configuration Manager console before you share distribution points from a source site. After you share distribution points, only the distribution points that are successfully shared are listed.

After you have shared distribution points, you can change the configuration of any shared distribution point in the source hierarchy. Changes that you make to the configuration of a distribution point are reflected in the destination hierarchy after the next data gathering cycle. Distribution points that you updated to qualify for sharing are shared automatically, while those that no longer qualify stop sharing distribution points. For example, you might have a distribution point that is not set up with an intranet FQDN and was not initially shared with the destination hierarchy. After you set up the FQDN for that distribution point, the next data gathering cycle identifies this configuration, and the distribution point is then shared with the destination hierarchy.

Plan to upgrade Configuration Manager 2007 shared distribution points

When you migrate from a Configuration Manager 2007 source hierarchy, you can upgrade a shared distribution point to make it a System Center Configuration Manager distribution point. You can upgrade distribution points at primary sites and secondary sites. The upgrade process removes the distribution point from the Configuration Manager 2007 hierarchy and makes it a site system server in the destination hierarchy. This process also copies the existing content that is on the distribution point to a new location on the distribution point computer. The upgrade process then modifies the copy of the content to create the single instance store for use with content deployment in the destination hierarchy. Therefore, when you upgrade a distribution point, you do not have to redistribute migrated content that was hosted on the Configuration Manager 2007 distribution point.

After Configuration Manager converts the content to the single instance store, Configuration Manager deletes the original source content on the distribution point computer to free up disk space. Configuration Manager does not use the original source content location.

Not all Configuration Manager 2007 distribution points that you can share are eligible for upgrade to System Center Configuration Manager. To be eligible for upgrade, a Configuration Manager 2007 distribution point must meet the conditions for upgrade. These conditions include the site system server on which the distribution point is installed and the type of Configuration Manager 2007 distribution point that is installed. For example, you cannot upgrade any type of distribution point that is installed on the site server computer at a primary site, but you can upgrade a standard distribution point that is installed on the site server computer at a secondary site.

NOTE

You can upgrade only those Configuration Manager 2007 shared distribution points that are on a computer that runs an operating system version that is supported for distribution points in the destination hierarchy. For example, although you can share a Configuration Manager 2007 distribution point that is on a computer that runs Windows Vista, you cannot upgrade this shared distribution point because the operating system is not supported by System Center Configuration Manager for use as a distribution point.

The following table lists the supported locations for each type of Configuration Manager 2007 distribution point that you can upgrade.

TYPE OF DISTRIBUTION POINT	DISTRIBUTION POINT ON A SITE SYSTEM COMPUTER OTHER THAN THE SITE SERVER	DISTRIBUTION POINT ON A SITE SYSTEM COMPUTER OTHER THAN THE SITE SERVER AND HOSTING OTHER SITE SYSTEM ROLES	DISTRIBUTION POINT ON A SECONDARY SITE SERVER
Standard distribution point	Yes	No	Yes
Distribution point on server shares[1]	Yes	No	No
Branch distribution point	Yes	No	No

[1] System Center Configuration Manager does not support server shares for site systems, but it does support the upgrade of a Configuration Manager 2007 distribution point that is on a server share. When you upgrade a Configuration Manager 2007 distribution point that is on a server share, the distribution point type is automatically converted to a server, and you must select the drive on the distribution point computer that will store the single instance content store.

WARNING

Before you upgrade a branch distribution point, uninstall the Configuration Manager 2007 client software. When you upgrade a branch distribution point that has the Configuration Manager 2007 client software installed, the content that was previously deployed to the computer is removed from the computer, and the upgrade of the distribution point fails.

To identify distribution points that are eligible for upgrade in the Configuration Manager console in the **Source Hierarchy** node, select a source site, and then select the **Shared Distribution Points** tab. Eligible distribution points display **Yes** in the **Eligible for Upgrade** column.

When you upgrade a distribution point that is installed on a Configuration Manager 2007 secondary site server, the secondary site is uninstalled from the source hierarchy. Although this scenario is called a secondary site upgrade, this applies only to the distribution point site system role. The result is that the secondary site is not upgraded and instead is uninstalled. This leaves a distribution point from the destination hierarchy on the computer that was the secondary site server. If you plan to upgrade the distribution point on a secondary site, see Plan to upgrade Configuration Manager 2007 secondary sites in this topic.

Distribution point upgrade process

You can use the Configuration Manager console to upgrade Configuration Manager 2007 distribution points that you have shared with the destination hierarchy. When you upgrade a shared distribution point, the distribution point is uninstalled from the Configuration Manager 2007 site. It is then installed as a distribution point that is attached to a primary or secondary site that you specify in the destination hierarchy. The upgrade process creates a copy of the migrated content that is stored on the distribution point, and then converts this copy to the single instance content store. When Configuration Manager converts a package to the single instance content store, it

deletes that package from the SMSPKG share on the distribution point computer unless the package has one or more advertisements that are set to **Run program from distribution point**.

To upgrade the distribution point, Configuration Manager uses the **Source Site Access Account** that is set up to gather data from the SMS Provider of the source site. Although this account requires only **Read** permission for site objects to gather data from the source site, it must also have **Delete** and **Modify** permission to the **Site** class to successfully remove the distribution point from the Configuration Manager 2007 site during the upgrade.

> **NOTE**
> Configuration Manager can convert content to the single instance store on only one distribution point at a time. When you set up multiple distribution point upgrades, the distribution points are queued for upgrade and processed one at a time.

Before you upgrade a shared distribution point, ensure that all content that is deployed to the distribution point is migrated. Content that you do not migrate before you upgrade the distribution point is not available in the destination hierarchy after the upgrade. When you upgrade a distribution point, the content in the migrated packages is converted into a format that is compatible with the single instance store of the destination hierarchy.

To upgrade a distribution point from within the Configuration Manager console, the Configuration Manager 2007 site system server must meet the following conditions:

- The distribution point configuration and location must be eligible for upgrade.
- The distribution point computer must have sufficient disk space for the content to be converted from the Configuration Manager 2007 content storage format to the single instance store format. This conversion requires available free disk space equal to the size of the largest package that is stored on the distribution point.
- The distribution point computer must run an operating system version that is supported as a distribution point in the destination hierarchy.

  > **NOTE**
  > When Configuration Manager checks for the eligibility of a distribution point for upgrade, it does not validate the operating system version of the distribution point computer.

To upgrade a distribution point, in the **Administration** workspace, expand **Migration**, expand the **Source Hierarchy** node, and then select the site that has the distribution point that you want to upgrade. Next, in the details pane, on the **Shared Distribution Points** tab, select the distribution point that you want to upgrade.

You can confirm that the distribution point is ready for upgrade by viewing the status in the **Eligible for Reassignment** column. Next, on the Configuration Manager console ribbon, on the **Distribution Points** tab, in the **Distribution Point** group, select **Reassign**. This opens a wizard that you use to finish the upgrade of the distribution point.

When you upgrade a shared distribution point, you must assign the distribution point to a primary or secondary site of your choice in the destination hierarchy. After the distribution point is upgraded, manage the distribution point as a distribution point in the destination hierarchy like any other distribution point.

You can monitor the progress of a distribution point upgrade in the Configuration Manager console by selecting the **Distribution Point Migration** node under the **Migration** node of the **Administration** workspace. You can also view information in the **Migmctrl.log** on the central administration site server of the destination hierarchy, or in the **distmgr.log** on the site server in the destination hierarchy that manages the upgraded distribution point.

> **NOTE**
>
> When you upgrade a distribution point to the destination hierarchy, the distribution point site system role is removed from the Configuration Manager 2007 source site. However, packages that were sent to the distribution point are not updated in the Configuration Manager 2007 hierarchy. In the Configuration Manager 2007 console, packages that had been sent to the distribution point continue to list the site system computer as a distribution point with a **Type** of **Unknown**. Subsequent updates to the package in Configuration Manager 2007 result in Distribution Manager reporting errors in the distmgr.log for that site when the site attempts to update the package on the unknown site system.

If you decide not to upgrade a shared distribution point, you can still install a distribution point from the destination hierarchy on a former Configuration Manager 2007 distribution point. Before you can install the new distribution point, you must first uninstall all Configuration Manager 2007 site system roles from the distribution point computer. This includes the Configuration Manager 2007 site if it is the site server computer. When you uninstall a Configuration Manager 2007 distribution point, content that was deployed to the distribution point is not deleted from the computer.

Plan to upgrade Configuration Manager 2007 secondary sites

When you use migration to upgrade a shared distribution point that is hosted on a Configuration Manager 2007 secondary site server, Configuration Manager upgrades the distribution point site system role to be a distribution point in the destination hierarchy. It also uninstalls the secondary site from the source hierarchy. The result is a System Center Configuration Manager distribution point, but no secondary site.

For a distribution point on the site server computer to be eligible for upgrade, Configuration Manager must be able to uninstall the secondary site and each of the site system roles on that computer. Typically, a shared distribution point on a Configuration Manager 2007 server share is eligible for upgrade. However, when a server share exists on the secondary site server, the secondary site and any shared distribution points on that computer are not eligible for upgrade. This is because the server share is treated as an additional site system object when the process attempts to uninstall the secondary site, and this process cannot uninstall this object. In this scenario, you can enable a standard distribution point on the secondary site server and then redistribute the content to that standard distribution point. This process does not use network bandwidth, and when finished, you can uninstall the distribution point on the server share, remove the server share, and then upgrade the distribution point and secondary site.

Before you upgrade a shared distribution point, review the distribution point configuration in Configuration Manager 2007 to avoid upgrading a distribution point on a secondary site that you still want to use with Configuration Manager 2007. This is a good practice, because after you upgrade a shared distribution point that is on a secondary site server, the site system server is removed from the Configuration Manager 2007 hierarchy and is no longer available for use with that hierarchy. When the secondary site is removed, any remaining distribution points at that secondary site are orphaned. This means they become unmanaged from Configuration Manager 2007 and are no longer shared or eligible for upgrade.

> **WARNING**
>
> When you view shared distribution points in the Configuration Manager console, there is no visible indication that a shared distribution point is on a remote site system server or on the secondary site server.

When you have a secondary site in a remote network location that is used primarily to control the deployment of content to that remote location, consider upgrading secondary sites that have a shared distribution point. Because you can set up bandwidth control for when you distribute content to a System Center Configuration Manager distribution point, you can often upgrade a secondary site to a distribution point, set up the distribution point for bandwidth controls, and avoid installing a secondary site in that network location in the destination hierarchy.

The process to upgrade a shared distribution point on a secondary site server is the same as any other shared

distribution point upgrade. Content is copied and converted to the single instance store in use by the destination hierarchy. However, when you upgrade a shared distribution point that is on a secondary site server, the upgrade process also uninstalls the management point (if present) and then uninstalls the secondary site from the server. The result is that the secondary site is removed from the Configuration Manager 2007 hierarchy. To uninstall the secondary site, Configuration Manager uses the account that is set up to gather data from the source site.

During the upgrade, there is a delay between when the Configuration Manager 2007 secondary site is uninstalled and the when the installation of the distribution point in the destination hierarchy begins. The data-gathering cycle determines this delay of up to four hours. The delay is intended to provide time for the secondary site to uninstall before the new distribution point installation begins.

For more about how to upgrade a shared distribution point, see Plan to upgrade Configuration Manager 2007 shared distribution points.

Plan to reassign System Center Configuration Manager distribution points

When you migrate from a supported version of System Center 2012 Configuration Manager to a hierarchy of the same version, you can reassign a shared distribution point from the source hierarchy to a site in the destination hierarchy. This is like the concept of upgrading a Configuration Manager 2007 distribution point to become a distribution point in the destination hierarchy. You can reassign distribution points from primary sites and secondary sites. The action to reassign a distribution point removes the distribution point from the source hierarchy and makes the computer and its distribution point a site system server of the site that you select in the destination hierarchy.

When you reassign a distribution point, you do not have to redistribute migrated content that was hosted on the source site distribution point. Additionally, unlike the upgrade of a Configuration Manager 2007 distribution point, reassignment of a distribution point does not require additional disk space on the distribution point computer. This is because beginning with System Center 2012 Configuration Manager, distribution points use the single instance store format for content. The content on the distribution point computer does not need to be converted when the distribution point is reassigned between hierarchies.

For a System Center 2012 Configuration Manager distribution point to be eligible for reassignment, it must meet the following criteria:

- A shared distribution point must be installed on a computer other than the site server.
- A shared distribution point cannot be co-located with any additional site system roles.

To identify distribution points that are eligible for reassignment in the Configuration Manager console in the **Source Hierarchy** node, select a source site, and then select the **Shared Distribution Points** tab. Eligible distribution points display **Yes** in the **Eligible for Reassignment** column (this column is named **Eligible for Upgrade** prior to System Center 2012 R2 Configuration Manager).

Distribution point reassignment process

You can use the Configuration Manager console to reassign distribution points that you have shared from an active source hierarchy. When you reassign a shared distribution point, the distribution point is uninstalled from its source site and then installed as a distribution point that is attached to a primary or secondary site that you specify in the destination hierarchy.

To reassign the distribution point, the destination hierarchy uses the Source Site Access Account that is set up to gather data from the SMS Provider of the source site. For information about required permissions and additional prerequisites, see Prerequisites for migration in System Center Configuration Manager.

Migrate multiple shared distribution points at the same time

Beginning with version 1610, you can use **Reassign Distribution point** to have Configuration Manager process in parallel the reassignment of up to 50 shared distribution points at the same time. This includes shared distribution points from supported source sites that run:

- Configuration Manager 2007
- System Center 2012 Configuration Manager
- System Center 2012 R2 Configuration Manager
- System Center Configuration Manager (Current Branch)

When you reassign distribution points, each distribution point must qualify to be either upgraded or reassigned. The name of the action and process involved (upgrade or reassign) depends on which version of Configuration Manager the source site runs. The end results for both actions are the same: the distribution point is assigned to one of your Current Branch sites with its content in place.

Prior to version 1610, Configuration Manager could process only one distribution point at a time. Now you can reassign as many distribution points as you want with the following caveats:

- Although you cannot multiselect distribution points to be reassigned, when you have queued up more than one, Configuration Manager will process them in parallel instead of waiting to finish one before starting the next.
- By default, up to 50 distribution points are processed in parallel at a time. After the reassignment of the first distribution point is finished, Configuration Manager will begin to process the 51st, and so on.
- When you use the Configuration Manager SDK, you can change **SharedDPImportThreadLimit** to adjust the number of reassigned distribution points that Configuration Manager can process in parallel.

Assign content ownership when migrating content

When you migrate content for deployments, you must assign the content object to a site in the destination hierarchy. This site then becomes the owner for that content in the destination hierarchy. Although the top-level site of your destination hierarchy is the site that migrates the metadata for content, it is the assigned site that uses the original source files for the content across the network.

To minimize the network bandwidth that is used when you migrate content, consider transferring ownership of content to a site in the destination hierarchy that is close on the network to the content location in the source hierarchy. Because information about the content in the destination hierarchy is shared globally, it will be available at every site.

Although information about content is shared to all sites by using database replication, any content that you assign to a primary site and then deploy to distribution points at other primary sites transfers by file-based replication. This transfer is routed through the central administration site and then to the additional primary site. You can reduce data transfers across low-bandwidth networks by centralizing packages that you plan to distribute to multiple primary sites before or during migration when you assign a site as the content owner.

Plan for the migration of Configuration Manager objects to System Center Configuration Manager

9/11/2019 • 12 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

With System Center Configuration Manager, you can migrate many of the different objects that are associated with different features found at a source site. Use the following sections to help you plan for the migration of objects between hierarchies.

- Plan to migrate software updates
- Plan to migrate content
- Plan to migrate collections
- Plan to migrate operating system deployments
- Plan to migrate desired configuration management
- Plan to migrate boundaries
- Plan to migrate reports
- Plan to migrate organizational and search folders
- Plan to migrate Asset Intelligence customizations
- Plan to migrate software metering rules customizations

Plan to migrate software updates

You can migrate software update objects, like software update packages and software update deployments.

To successfully migrate software update objects, you must first set up your destination hierarchy with configurations that match your source hierarchy environment. This requires the following actions:

- Deploy an active software update point in the destination hierarchy
- Set up the catalog of products and languages to match the configuration of your source hierarchy
- Sync the software update point in the destination hierarchy with Windows Server Update Services (WSUS)

When you migrate software updates, consider the following:

- Migration of software update objects can fail when you have not synced information in your destination hierarchy to match the configuration of your source hierarchy.

  > **WARNING**
  > Configuration Manager does not support use of the WSUSutil tool to sync data between a source and destination hierarchy.

- You cannot migrate custom updates that are published by using System Center Updates Publisher. Instead, custom updates must be republished to the destination hierarchy.

When you migrate from a Configuration Manager 2007 source hierarchy, the migration process modifies some software update objects to the format in use by the destination hierarchy. Use the following table to help you plan the migration of software update objects from Configuration Manager 2007.

CONFIGURATION MANAGER 2007 OBJECT	OBJECT NAME AFTER MIGRATION
Software update lists	Software update lists are converted to software update groups.
Software update deployments	Software update deployments are converted to deployments and update groups. After you migrate a software update deployment from Configuration Manager 2007, you must enable it in the destination hierarchy before you can deploy it.
Software update packages	Software update packages remain software update packages.
Software update templates	Software update templates remain software update templates. The **Duration** value in Configuration Manager 2007 deployment templates does not migrate.

When you migrate objects from a System Center 2012 Configuration Manager or System Center Configuration Manager source hierarchy, the software updates objects are not modified.

Plan to migrate content

You can migrate content from a supported source hierarchy to your destination hierarchy. For a Configuration Manager 2007 source hierarchy, this content includes software distribution packages and programs and virtual applications, like Microsoft Application Virtualization (App-V). For System Center 2012 Configuration Manager and System Center Configuration Manager source hierarchies, this content includes applications and App-V virtual applications. When you migrate content between hierarchies, the compressed source files migrate to the destination hierarchy.

Packages and programs

When you migrate packages and programs, they are not modified by migration. However, before you migrate them, you must set up each package to use a Universal Naming Convention (UNC) path for its source file location. As part of the configuration to migrate packages and programs, you must assign a site in the destination hierarchy to manage this content. The content is not migrated from the assigned site, but after migration, the assigned site accesses the original source file location by using the UNC mapping.

After you migrate a package and program to the destination hierarchy, and while migration from the source hierarchy remains active, you can make the content available to clients in that hierarchy by using a shared distribution point. To use a shared distribution point, the content must remain accessible on the distribution point at the source site. For more about shared distribution points, see Share distribution points between source and destination hierarchies in Plan a content deployment migration strategy in System Center Configuration Manager.

For content that has migrated, if the content version changes in the source hierarchy or the destination hierarchy, clients can no longer access the content from the shared distribution point in the destination hierarchy. In this scenario, you must re-migrate the content to restore a consistent version of the package between the source hierarchy and the destination hierarchy. This information syncs during the data gathering cycle.

TIP

For each package that you migrate, update the package in the destination hierarchy. This action can prevent issues with deploying the package to distribution points in the destination hierarchy. However, when you update a package on the distribution point in the destination hierarchy, clients in that hierarchy will no longer be able to get that package from a shared distribution point. To update a package in the destination hierarchy, in the Configuration Manager console, go to the Software Library, right-click on the package, and then select **Update Distribution Points**. Do this action for each package that you migrate.

TIP

You can use Microsoft System Center Configuration Manager Package Conversion Manager to convert packages and programs into System Center Configuration Manager applications. Download Package Conversion Manager from the Microsoft Download Center site. For more information, see Configuration Manager Package Conversion Manager.

Virtual applications

When you migrate App-V packages from a supported Configuration Manager 2007 site, the migration process converts them to applications in the destination hierarchy. Additionally, based on existing advertisements for the App-V package, the following deployment types are created in the destination hierarchy:

- If there are no advertisements, one deployment type is created that uses the default deployment type settings.
- If one advertisement exists, one deployment type is created that uses the same settings as the Configuration Manager 2007 advertisement.
- If multiple advertisements exist, a deployment type is created for each Configuration Manager 2007 advertisement by using the settings for that advertisement.

IMPORTANT

If you migrate a previously migrated Configuration Manager 2007 App-V package, the migration fails because virtual application packages do not support the overwrite migration behavior. In this scenario, you must delete the migrated virtual application package from the destination hierarchy, and then create a new migration job to migrate the virtual application.

NOTE

After you migrate an App-V package, you can use the Update Content wizard to change the source path for App-V deployment types. For more about how to update content for a deployment type, see How to manage deployment types in Management tasks for System Center Configuration Manager applications.

When you migrate from a System Center 2012 Configuration Manager or System Center Configuration Manager source hierarchy, you can migrate objects for the App-V virtual environment in addition to App-V deployment types and applications. For more about App-V environments, see Deploying App-V virtual applications with System Center Configuration Manager.

Advertisements

You can migrate advertisements from a supported Configuration Manager 2007 source site to the destination hierarchy by using collection-based migration. If you upgrade a client, it retains the history of previously run advertisements to prevent the client from rerunning migrated advertisements.

> **NOTE**
> You cannot migrate advertisements for virtual packages. This is an exception to the migration of advertisements.

Applications

You can migrate applications from a supported System Center 2012 Configuration Manager or System Center Configuration Manager source hierarchy to a destination hierarchy. If you reassign a client from the source hierarchy to the destination hierarchy, the client retains the history of previously installed applications to prevent the client from rerunning a migrated application.

Plan to migrate collections

You can migrate the criteria for collections from a supported System Center 2012 Configuration Manager or System Center Configuration Manager source hierarchy. For this, you use an object-based migration job. When you migrate a collection, you migrate the rules for the collection and not information about the members of the collection or information or objects related to the members of the collection.

Migration of the collection object is not supported when you migrate from a Configuration Manager 2007 source hierarchy.

Plan to migrate operating system deployments

You can migrate the following operating system deployment objects from a supported source hierarchy:

- Operating system images and packages. The source path of boot images is updated to the default image location for the Windows Administrative Installation Kit (Windows AIK) on the destination site. The following are requirements and limitations to migrating operating system images and packages:
  - To successfully migrate image files, the computer account of the SMS Provider server for the destination hierarchy's top-level site must have **Read** and **Write** permission to the image source files of the source site's Windows AIK location.
  - When you migrate an operating system installation package, ensure that the configuration of the package on the source site points to the folder that has the WIM file and not to the WIM file itself. If the installation package points to the WIM file, the migration of the installation package will fail.
  - When you migrate a boot image package from a Configuration Manager 2007 source site, the package ID of the package is not maintained in the destination site. The result of this is that clients in the destination hierarchy cannot use boot image packages that are available on shared distribution points.
- Task sequences. When you migrate a task sequence that has a reference to a client installation package, that reference is replaced with a reference to the client installation package of the destination hierarchy.

  > **NOTE**
  > When you migrate a task sequence, Configuration Manager might migrate objects that are not required in the destination hierarchy. These objects include boot images and Configuration Manager 2007 client installation packages.

- Drivers and driver packages. When you migrate driver packages, the computer account of the SMS Provider in the destination hierarchy must have full control to the package source.

Plan to migrate desired configuration management

You can migrate configuration items and configuration baselines.

> **NOTE**
>
> Uninterpreted configuration items from Configuration Manager 2007 source hierarchies are not supported for migration. You cannot migrate or import these configuration items to the destination hierarchy. For more about uninterpreted configuration items, see Uninterpreted configuration items in the About Configuration Items in Desired Configuration Management topic in the Configuration Manager 2007 documentation library.

You can import Configuration Manager 2007 Configuration Packs. The import process automatically converts the configuration packs to be compatible with System Center Configuration Manager.

Plan to migrate boundaries

You can migrate boundaries between hierarchies. When you migrate boundaries from Configuration Manager 2007, each boundary from the source site migrates at the same time and is added to a new boundary group that is created in the destination hierarchy. When you migrate boundaries from a System Center 2012 Configuration Manager or System Center Configuration Manager hierarchy, each boundary you select is added to a new boundary group in the destination hierarchy.

Each automatically created boundary group is enabled for content location but not for site assignment. This prevents overlapping boundaries for site assignment between the source and destination hierarchies. When you migrate from a Configuration Manager 2007 source site, this helps prevent new Configuration Manager 2007 clients that install from incorrectly assigning to the destination hierarchy. By default, System Center Configuration Manager clients do not automatically assign to Configuration Manager 2007 sites.

During migration, if you share a distribution point with the destination hierarchy, any boundaries that are associated with that distribution automatically migrate to the destination hierarchy. In the destination hierarchy, migration creates a new read-only boundary group for each shared distribution point. If you change the boundaries for the distribution point in the source hierarchy, the boundary group in the destination hierarchy updates with these changes during the next data gathering cycle.

Plan to migrate reports

Configuration Manager does not support the migration of reports. Instead, use SQL Server Reporting Services Report Builder to export reports from the source hierarchy, and then import them to the destination hierarchy.

> **NOTE**
>
> Because there are schema changes for reports between Configuration Manager 2007 and System Center Configuration Manager, test each report that you import from a Configuration Manager 2007 hierarchy to ensure that it functions as expected.

For more about reporting, see Reporting in System Center Configuration Manager.

Plan to migrate organizational and search folders

You can migrate organizational folders and search folders from a supported source hierarchy to a destination hierarchy. In addition, from a System Center 2012 Configuration Manager or System Center Configuration Manager source hierarchy, you can migrate the criteria for a saved search to a destination hierarchy.

By default, the migration process maintains your search folder and administrative folder structures for objects and collections when you migrate. However, in the Create Migration Job wizard, on the **Settings** page, you can set up a migration job to not migrate the organizational structure for objects by unchecking the box for this option. The

organizational structures of collections are always maintained.

One exception to this is a search folder that contains virtual applications. When an App-V package is migrated, the App-V package is transformed into an application in System Center Configuration Manager. After migration of the search folder, only the remaining packages are found, and the search folder cannot locate an App-V package because of this conversion to an application when the App-V package migrates.

When you migrate a saved search from a System Center 2012 Configuration Manager or System Center Configuration Manager source hierarchy, you migrate the criteria for the search, and not the information about the search results. Migration of a saved search is not applicable from a Configuration Manager 2007 source site.

Plan to migrate Asset Intelligence customizations

You can migrate customizations for Asset Intelligence from a supported source hierarchy to a destination hierarchy. There are no significant changes to the structure of Asset Intelligence customizations between Configuration Manager 2007 and System Center Configuration Manager.

> **NOTE**
> System Center Configuration Manager does not support the migration of Asset Intelligence objects from a Configuration Manager 2007 site that is using Asset Intelligence Service 2.0 (AIS 2.0).

Plan to migrate software metering rules customizations

There are no significant changes to software metering between Configuration Manager 2007 and System Center Configuration Manager. You can migrate your software metering rules from a supported source hierarchy to a destination hierarchy.

By default, software metering rules that you migrate to a destination hierarchy are not associated with a specific site in the destination hierarchy and instead apply to all clients in the hierarchy. To apply a software metering rule to clients at a specific site, you must edit the metering rule after it migrates.

Planning to monitor migration activity in System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

With System Center Configuration Manager, you can monitor migration in the Configuration Manager console that connects to the destination hierarchy. In the Configuration Manager console in the **Administration** workspace, you can use the **Migration** node to monitor the progress and success of migration jobs. You can view summary information for each migration job that identifies objects that have migrated, those objects that have not yet migrated, and the number of objects that are excluded from a migration job. You will also see details about any migration problems.

View Migration Progress

To view the progress of a migration job, use any of the following actions:

- In the **Administration** workspace of the Configuration Manager console, expand the **Migration Jobs** node, select a migration job, and then select the **Objects in Job** tab.
- Use the Configuration Manager log files to review the migration progress or to identify any problems. Migration Manager is the Configuration Manager process that tracks migration actions and records these in the migmctrl.log file in the **<InstallationPath>\LOGS** folder on the site server.

  > **NOTE**
  > If a migration job fails, review the details in the migmctrl.log file as soon as possible. The migration log entries are continually added to the file and overwrite old details. If the entries are overwritten, you might not be able to identify whether any problems that you might encounter with the migrated objects relate to migration issues. Migration activity is logged at the top-level site of the hierarchy regardless of the site your Configuration Manager console connects to when you configure migration.

- Use Configuration Manager reporting. Configuration Manager provides several built-in reports for migration, or you can edit those reports to fit your requirements. For more information about Configuration Manager reports, see Reporting in System Center Configuration Manager.

Plan to complete migration in System Center Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

With System Center Configuration Manager, you can complete the process of migration when a source hierarchy no longer has data that you want to migrate to your destination hierarchy. Completing migration includes the following general steps:

- Ensure that data you require has migrated. Before you complete migration from a source hierarchy, make sure that you have successfully migrated all of the resources from the source hierarchy that you require in the destination hierarchy. This can include data and clients.
- Stop gathering data from source sites. To complete migration from a source hierarchy, you must first stop gathering data from source sites.
- Clean up migration data. After you stop gathering data from all source sites in a source hierarchy, you can remove data about the migration process and source hierarchy from the database of the destination hierarchy.
- Decommission the source hierarchy. After you complete migration from a source hierarchy and that hierarchy no longer has resources that you manage, you can decommission the sites in the source hierarchy and remove the related infrastructure from your environment. For information about how to decommission sites and source hierarchies, consult the documentation for that version of Configuration Manager.

Use the following sections to help you plan to complete migration from a source hierarchy by stopping data gathering and cleaning up migration data:

- Plan to stop gathering data
- Plan to clean up migration data

Plan to stop gathering data

Before you complete migration and clean up migration data, you must stop gathering data from each source site in the source hierarchy. To stop gathering data from each source site, you must perform the **Stop Gathering Data** command on the bottom tier source sites, and then repeat the process at each parent site. The top-level site of the source hierarchy must be the last site on which you stop gathering data. You must stop data gathering at each child site before performing this command on a parent site. Typically, you only stop gathering data when you are ready to finish the migration process.

After you stop gathering data from a source site, shared distribution points from that site are no longer available as content locations for clients in the destination hierarchy. Therefore, ensure that any migrated content that the clients in the destination hierarchy require access to remains available by using one of the following options:

- In the destination hierarchy, distribute the content to at least one distribution point.
- Before you stop gathering data from a source site, upgrade or reassign shared distribution points that have the required content. For more about upgrading or reassigning shared distribution points, see the applicable sections in Planning a content deployment migration strategy in System Center Configuration Manager.

After you stop gathering data from each source site in the source hierarchy, you can clean up migration data. Until you clean up migration data, each migration job that has run or that is scheduled to run remains accessible in the Configuration Manager console.

For more about source sites and data gathering, see Planning a source hierarchy strategy in System Center Configuration Manager.

Plan to clean up migration data

The last step required to finish migration is to clean up migration data. You can use the **Clean Up Migration Data** command after you have stopped gathering data for each source site in the source hierarchy. This optional action removes data about the current source hierarchy from the database of the destination hierarchy.

When you clean up migration data, most data about the migration is removed from the database of the destination hierarchy. However, details about migrated objects are retained. With these details, you can use the **Migration** workspace to reconfigure the source hierarchy that has the data that was migrated to resume migration from that source hierarchy, or to review the objects and site ownership of the objects that previously migrated.

Configure source hierarchies and source sites for migration to System Center Configuration Manager

2/12/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To enable migration of data to your System Center Configuration Manager environment, you must configure a supported Configuration Manager source hierarchy and one or more source sites in that hierarchy that contain data that you want to migrate.

> **NOTE**
> Operations for migration are run at the top-level site in the destination hierarchy. If you configure migration when you use a Configuration Manager console that is connected to a primary child site, you must allow time for the configuration to replicate to the central administration site, start, and then replicate status back to the primary site to which you are connected.

Use the information and procedures in the following sections to specify the source hierarchy and add additional source sites. After you finish these procedures, you can create migration jobs and start to migrate data from the source hierarchy to the destination hierarchy.

- Specify a source hierarchy for migration
- Identify additional source sites of the source hierarchy

Specify a source hierarchy for migration

To migrate data to your destination hierarchy, you must specify a supported source hierarchy that has the data that you want to migrate. By default, the top-level site of that hierarchy becomes a source site of the source hierarchy. If you migrate from a Configuration Manager 2007 hierarchy, you can then set up additional source sites for migration after data is gathered from the initial source site. If you migrate from a System Center 2012 Configuration Manager or System Center Configuration Manager hierarchy, you do not have to set up additional source sites to migrate data from the source hierarchy. This is because these versions of Configuration Manager use a shared database that is available at the top-level site of the source hierarchy. The shared database has all the information that you can migrate.

Use the following procedures to specify a source hierarchy for migration and to identify additional source sites in a Configuration Manager 2007 hierarchy.

Run this procedure with a Configuration Manager console that is connected to the destination hierarchy:

To configure a source hierarchy

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Migration**, and then click **Source Hierarchy**.
3. On the **Home** tab, in the **Migration** group, click **Specify Source Hierarchy**.
4. In the **Specify Source Hierarchy** dialog box, for **Source Hierarchy**, select **New source hierarchy**.
5. For **Top-level Configuration Manager site server**, enter the name or IP address of the top-level site of a supported source hierarchy.

6. Specify source site access accounts that have the following permissions:

   - Source Site Account: **Read** permission to the SMS Provider for the specified top-level site in the source hierarchy. Distribution point sharing and upgrades require **Modify** and **Delete** permissions to the site in the source hierarchy.
   - Source Site Database Account: **Read** and **Execute** permission to the SQL Server database for the specified top-level site in the source hierarchy.

     If you specify the use of the computer account, Configuration Manager uses the computer account of the top-level site of the destination hierarchy. For this option, ensure that this account is a member of the security group **Distributed COM Users** in the domain where the top-level site of the source hierarchy resides.

7. To share distribution points between the source and destination hierarchies, select the **Enable distribution point sharing for the source site server** check box. If you do not enable distribution point sharing at this time, you can do so by editing the credentials of the source site after data gathering has finished.
8. Click **OK** to save the configuration. This opens the **Data Gathering Status** dialog box, and data gathering starts automatically.
9. When data gathering finishes, click **Close** to close the **Data Gathering Status** dialog box and complete the configuration.

Identify additional source sites of the source hierarchy

When you configure a supported source hierarchy, the top-level site of that hierarchy is automatically configured as a source site, and data is automatically gathered from that site. The next action that you take depends on the version of Configuration Manager that is run by the source hierarchy:

- For a Configuration Manager 2007 source hierarchy, you can begin migration from that initial source site or set up additional source sites from the source hierarchy after the data gathering finishes for the initial source site. To migrate data that is only available from a child site, set up additional source sites for a Configuration Manager 2007 hierarchy. For example, you might configure additional source sites to gather data about content that you want to migrate when it's created at a child site in the source hierarchy and is not available at the top site of the source hierarchy.
- For a System Center 2012 Configuration Manager or System Center Configuration Manager source hierarchy, you do not need to configure additional source sites. This is because these versions of Configuration Manager use a shared database that is available at the top-level site of the source hierarchy. The shared database has all the information that you can migrate from all of the sites in that source hierarchy. This makes the data that you can migrate available from the top-level site of the source hierarchy.

When you configure additional source sites for a Configuration Manager 2007 source hierarchy, you must configure the additional source sites from the top of the source hierarchy to the bottom. You must configure a parent site as a source site before you configure any of its child sites as source sites.

Use the following procedure to configure additional source sites for Configuration Manager 2007 source hierarchies:

To identify additional source sites in the source hierarchy

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Migration**, and then click **Source Hierarchy**.
3. Choose the site that you want to configure as a source site.
4. On the **Home** tab, in the **Source Site** group, click **Configure**.

5. In the **Source Site Credentials** dialog box, for the source site access accounts, specify accounts that have the following permissions:

   - Source Site Account: **Read** permission to the SMS Provider for the specified top-level site in the source hierarchy. Distribution point sharing and upgrades require **Modify** and **Delete** permissions to the site in the source hierarchy.
   - Source Site Database Account: **Read** and **Execute** permission to the SQL Server database for the specified top-level site in the source hierarchy.

   If you specify the use of the computer account, Configuration Manager uses the computer account of the top-level site of the destination hierarchy. For this option, ensure that this account is a member of the security group **Distributed COM Users** in the domain where the top-level site of the source hierarchy resides.

6. To share distribution points between the source and destination hierarchies, select the **Enable distribution point sharing for the source site server** check box. If you do not enable distribution point sharing at this time, you can do so by editing the credentials for the source site after data gathering has finished.

7. Click **OK** to save the configuration. This opens the **Data Gathering Status** dialog box, and data gathering starts automatically.

8. When data gathering finishes, click **Close** to complete the configuration.

Operations for migrating to System Center Configuration Manager

2/12/2019 • 9 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

For migration in System Center Configuration Manager, you can migrate data and clients after you successfully gather data from a source site in a supported source hierarchy. Use the information in the following sections to create and run migration jobs to migrate data and clients, and then finish the migration process.

- Create and edit migration jobs
- Run migration jobs
- Upgrade or reassign a shared distribution point
- Monitor migration activity in the Migration workspace
- Migrate clients
- Finish migration

Create and edit migration jobs

Use the following procedures to create data migration jobs, edit the exclusion list for collection-based migration jobs, set up shared distribution points, and edit migration job schedules.

> **NOTE**
> The following procedure for creating a migrating job that migrates by collections applies only to source hierarchies that run a supported version of Configuration Manager 2007. The collection-based migration job type is not available when you migrate from a System Center 2012 Configuration Manager or System Center Configuration Manager source hierarchy.

Create a migration job to migrate by collections

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Migration**, and then choose **Migration Jobs**.
3. On the **Home** tab, in the **Create** group, choose **Create Migration Job**.
4. On the **General** page of the Create Migration Job wizard, set up the following and then choose **OK**:
   - Specify a name for the migration job.
   - In the **Job type** drop-down list, select **Collection migration**.
5. On the **Select Collections** page, set up the following and then choose **Next**:
   - Select the collections that you want to migrate.
   - If you want to migrate only collections and not the objects that are associated with those collections, uncheck **Migrate objects that are associated with the specified collections**. If you uncheck this option, no associated objects are migrated in this job, and you can skip steps 6 and 7.
6. On the **Select Objects** page, uncheck any object types or specific available objects that you do not want to

migrate. By default, all associated object types and available objects are selected. Choose **Next**.

7. On the **Content Ownership** page, assign the ownership of content from each listed source site to a site in the destination hierarchy, and then choose **Next**.
8. On the **Security Scope** page, select one or more role-based administration security scopes to assign to the objects to migrate in this migration job, and then choose **Next**.
9. On the **Collection Limiting** page, set up a collection from the destination hierarchy to limit the scope of each listed collection, and then choose **Next**. If no collections are listed, choose **Next**.
10. On the **Site Code Replacement** page, assign a site code from the destination hierarchy to replace the Configuration Manager 2007 site code for each listed collection, and then choose **Next**. If no collections are listed, choose **Next**.
11. On the **Review Information** page, choose **Save To File** to save the displayed information for later viewing. When you are ready to continue, choose **Next**.
12. On the **Settings** page, set up when the migration job will run, choose any additional settings that you need for this migration job, and then choose **Next**.
13. Confirm the settings and finish the wizard.

Create a migration Job to migrate by objects

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Migration**, and then choose **Migration Jobs**.
3. On the **Home** tab, in the **Create** group, choose **Create Migration Job**.
4. On the **General** page of the Create Migration Job wizard, set up the following, and then choose **Next**:
   - Specify a name for the migration job.
   - In the **Job type** drop-down list, select **Object migration**.
5. On the **Select Objects** page, select the object types that you want to migrate. By default, all available objects are selected for each object type that you select.
6. On the **Content Ownership** page, assign the ownership of content from each listed source site to a site in the destination hierarchy, and then choose **Next**. If no source sites are listed, choose **Next**.
7. On the **Security Scope** page, select one or more role-based administration security scopes to assign to the objects in this migration job, and then choose **Next**.
8. On the **Review Information** page, choose **Save To File** to save the displayed information for later viewing. When you are ready to continue, choose **Next**.
9. On the **Settings** page, set up when the migration job will run and choose any additional settings that you need for this migration job. Then choose **Next**.
10. Confirm the settings and finish the wizard.

Create a migration job to migrate changed objects

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Migration**, and then choose **Migration Jobs**.
3. On the **Home** tab, in the **Create** group, choose **Create Migration Job**.
4. On the **General** page of the Create Migration Job wizard, set up the following and then choose **Next**:
   - Specify a name for the migration job.

- In the **Job type** drop-down list, select **Objects modified after migration**.

5. On the **Select Objects** page, select the object types that you want to migrate. By default, all available objects are selected for each object type that you select.
6. On the **Content Ownership** page, assign the ownership of content from each listed source site to a site in the destination hierarchy, and then choose **Next**. If no source sites are listed, choose **Next**.
7. On the **Security Scope** page, select one or more role-based administration security scopes to assign to the objects in this migration job, and then choose **Next**.
8. On the **Review Information** page, choose **Save To File** to save the displayed information for later viewing. When you are ready to continue, choose **Next**.
9. On the **Settings** page, set up when the migration job will run and choose any additional settings that you require for this migration job. Unlike the other migration job types, this migration job must overwrite the previously migrated objects in the System Center Configuration Manager database. Choose **Next**.
10. Confirm the settings and then finish the wizard.

Modify the exclusion list for migration

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, choose **Migration** to gain access to the exclusion list. You can also access the exclusion list from the **Source Hierarchy** or **Migration Jobs** node.
3. On the **Home** tab, in the **Migration** group, choose **Edit Exclusion List**.
4. In the **Edit Exclusion List** dialog box, select the excluded object that you want to remove from the exclusion list, and then choose **Remove**.
5. Choose **OK** to save the changes and finish the edit. To cancel current changes and restore all the objects that you have removed, choose **Cancel**, and then choose **No**. This will cancel the removal of the objects, and close the **Edit Exclusion List** dialog box.

Share distribution points from the source hierarchy

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Migration**, choose **Source Hierarchy**, and then select the source site that you want to set up.
3. On the **Home** tab, in the **Source Site** group, choose **Configure**.
4. On the **Source Site Credentials** dialog box, select **Enable distribution point sharing for the source site server**, and then choose **OK**.
5. When data gathering finishes, choose **Close**.

Change the schedule of a migration job

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Migration**, and then choose **Migration Jobs**.
3. Choose the migration job that you want to change. On the **Home** tab, in the **Properties** group, choose **Properties**.
4. In the properties of the migration job, select the **Settings** tab, change the run time for the migration job, and then choose **OK**.

Run migration jobs

Use the following procedure to run a migration job that has not yet started.

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Migration**, and then choose **Migration Jobs**.
3. Choose the migration job that you want to run. On the **Home** tab, in the **Migration Job** group, choose **Start**.
4. Choose **Yes** to start the migration job.

Upgrade or reassign a shared distribution point

You can upgrade a supported distribution point that is shared from a Configuration Manager 2007 source site (or reassign a supported distribution point that is shared from a System Center Configuration Manager source site) to be a distribution point in the destination hierarchy.

> **IMPORTANT**
> Before you upgrade a Configuration Manager 2007 branch distribution point, you must uninstall the Configuration Manager 2007 client software from the branch distribution point computer. If the Configuration Manager 2007 client software is installed when you attempt to upgrade the distribution point, the upgrade fails and content that was previously deployed to the branch distribution point is removed from the computer.

Caution

When you upgrade or reassign a shared distribution point, the distribution point site system role and site system computer are removed from the source site and added as a distribution point to the site in the destination hierarchy that you select.

Upgrade or reassign a shared distribution point

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Migration**, and then choose **Source Hierarchy**.
3. Select the site that owns the distribution point you want to upgrade, choose the **Shared Distribution Points** tab, and select the eligible distribution point that you want to upgrade or reassign.
4. On the **Distribution Point** tab, in the **Distribution Point** group, choose **Reassign**.
5. Specify settings in the Reassign Shared Distribution Point wizard like you are installing a new distribution point for the destination hierarchy, with the following addition:
   - On the **Content Conversion** page, review the guidance about the space required to convert the existing content. Then, on the **Drive Settings** page of the wizard, ensure that the drive of the distribution point computer that is selected has the required amount of free disk space.
6. Confirm the settings and then finish the wizard.

Monitor migration activity in the Migration workspace

Use the Configuration Manager console to monitor migration.

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Migration**, and then choose **Migration Jobs**.
3. Choose the migration job that you want to monitor.
4. View details and status about the selected migration job on the tabs for **Summary** and **Objects in Job**.

Migrate clients

After you migrate data for clients between hierarchies but before you finish migration, plan to migrate clients to the destination hierarchy. The migration of clients between hierarchies involves uninstalling the Configuration Manager client software from computers that are assigned to the source hierarchy, and then installing the Configuration Manager client software from the destination hierarchy. When you install the client from the destination hierarchy you also assign the client to a primary site in that hierarchy. For more about migrating clients, see Planning a client migration strategy in System Center Configuration Manager.

Finish migration

Use this procedure to finish migration from the source hierarchy.

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Migration**, and then choose **Source Hierarchy**.
3. For a Configuration Manager 2007 source hierarchy, select a source site that is at the bottom level of the source hierarchy. For a System Center 2012 Configuration Manager or System Center Configuration Manager source hierarchy, select the available source site.
4. On the **Home** tab, in the **Clean Up** group, choose **Stop Gathering Data**.
5. Choose **Yes** to confirm the action.
6. For a Configuration Manager 2007 source hierarchy, before you continue to the next step, repeat steps 3, 4, and 5. Go through these steps at each site in the hierarchy, from the bottom of the hierarchy to the top. For a System Center 2012 Configuration Manager or System Center Configuration Manager source hierarchy, continue to the next step.
7. On the **Home** tab, in the **Clean Up** group, choose **Clean Up Migration Data**.
8. On the **Clean Up Migration Data** dialog box, from the **Source hierarchy** drop-down list, select the site code and site server of the top-level site of the source hierarchy, and then choose **OK**.
9. Choose **Yes** to finish the migration process for the source hierarchy.

Security and privacy for migration to System Center Configuration Manager

9/5/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This topic contains security best practices and privacy information for migration to your System Center Configuration Manager environment.

Security Best Practices for Migration

Use the following security best practice for migration.

SECURITY BEST PRACTICE	MORE INFORMATION
Use the computer account for the Source Site SMS Provider Account and the Source Site SQL Server Account rather than a user account.	If you must use a user account for migration, remove the account details when migration is completed.
Use IPsec when you migrate content from a distribution point in a source site to a distribution point in your destination site.	Although the migrated content is hashed to detect tampering, if the data is modified while it is transferred, the migration will fail.
Restrict and monitor the administrative users who can create migration jobs.	The integrity of the database of the destination hierarchy depends upon the integrity of data that the administrative user chooses to import from the source hierarchy. In addition, this administrative user can read all data from the source hierarchy.

Security Issues for Migration

Migration has the following security issues:

- Clients that are blocked from a source site might successfully assign to the destination hierarchy before their client record is migrated.

  Although Configuration Manager retains the blocked status of clients that you migrate, the client can successfully assign to the destination hierarchy if assignment occurs before the migration of the client record is completed.

- Audit messages are not migrated.

When you migrate data from a source site to a destination site, you lose any auditing information from the source hierarchy.

Privacy Information for Migration

Migration discovers information from the site databases that you identify in a source infrastructure and stores this data to the database in the destination hierarchy. The information that System Center Configuration Manager can discover from a source site or hierarchy depends upon the features that were enabled in the source environment, as well as the management operations that were performed in that source environment.

For more information about security and privacy information, see one of the following topics:

- For more information about the privacy information for Configuration Manager 2007, see Security and Privacy for Configuration Manager 2007 in the Configuration Manager 2007 documentation library.
- For more information about the privacy information for System Center 2012 Configuration Manager, see Security and Privacy for System Center 2012 Configuration Manager in the System Center 2012 Configuration Manager documentation library.
- For more information about the privacy information for System Center Configuration Manager, see Security and privacy for System Center Configuration Manager.

You can migrate some or all of the supported data from a source site to a destination hierarchy.

Migration is not enabled by default and requires several configuration steps. Migration information is not sent to Microsoft.

Before you migrate data from a source hierarchy, consider your privacy requirements.

Deploy servers and roles

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

After you plan out your Configuration Manager site and hierarchy topology and are ready to get sites installed or upgraded, use the information in the following articles:

- Install Configuration Manager sites
- Upgrade to Configuration Manager
- Scenarios to streamline your installation of Configuration Manager
- Configure sites and hierarchies
- Migrate data between hierarchies

Where to get installation media for System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

If you have System Center Configuration Manager volume licenses with Software Assurance, or if you have purchased licenses for System Center Configuration Manager volume licenses, you can download baseline source media to install System Center Configuration Manager from the Volume Licensing Service Center.

If you have a System Center Configuration Manager license from EMS, Microsoft 365, or a Cloud Solution Provider (CSP), please see the Product and Licensing FAQ.

If you would like to purchase volume licenses for System Center Configuration Manager, contact your preferred Microsoft Reseller or see How to purchase through Volume Licensing. You can also download media to install an evaluation edition of System Center Configuration Manager from the TechNet Evaluation Center website.

To learn about baseline media for Configuration Manager, see Baseline and update versions.

Reference for System Center Configuration Manager Setup

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

System Center Configuration Manager Setup provides links to several topics that are detailed in the following sections. The information presented here can help you prepare to install a Configuration Manager site or hierarchy, and help prepare you for some of the decisions you must make during the installation.

Before you begin

Before you install new Configuration Manager sites, make sure you have reviewed the following information, which can help set the stage for a successful deployment design:

- Fundamentals of System Center Configuration Manager
- Plan for System Center Configuration Manager infrastructure
- Prepare to install System Center Configuration Manager sites

Assess server readiness

Before you begin the installation of a new site, make sure that the site server and the remote site system servers you plan to use for the site (for example, the server that hosts the site database) meet all prerequisite configurations. These topics in the documentation library can help:

- Supported configurations for System Center Configuration Manager
- Prerequisite Checker

Clients for additional operating systems

You can download client software for Configuration Manager from the Microsoft Download Center for the following operating systems:

- Mac (Apple)
- UNIX
- Linux

Use the following links to download clients for the version of Configuration Manager you use:

- See Microsoft System Center Configuration Manager - Clients for Additional Operating Systems

Usage data levels and settings

When you install your first System Center Configuration Manager site, Configuration Manager automatically installs and configures a new site system role, the **service connection point**, on the site server. The service connection point has these default settings:

- **Online** mode (an offline mode also is available)
- **Enhanced** data collection level (two other data collection levels, Basic and Full, also are available)

When the service connection point site system role is online, Microsoft can automatically collect diagnostics and

usage information over the Internet. Information that is collected helps us:

- Identify and troubleshoot problems
- Improve our products and service
- Identify updates for Configuration Manager that apply to the version of Configuration Manager you use

Levels of data collection

Data collection includes these three levels:

- **Basic** includes data about setup and upgrade, like the number of sites and which Configuration Manager features are enabled. No personally identifiable information is transmitted.
- **Enhanced** includes the data in the Basic level setting, plus it transmits data about the hierarchy, how each feature is used (frequency and duration), and enhanced diagnostic information like the memory state of your server when a system or app crash occurs. No personally identifiable data is transmitted.
- **Full** includes the data in the Basic and Enhanced level settings, and it also sends advanced diagnostic information like system files and memory snapshots. This option might include personally identifiable information, but we won't use that information to identify or contact you, or to target advertising to you.

For more information, including disclosure of the details collected by each level, see Diagnostics and usage data for System Center Configuration Manager.

To view the System Center Configuration Manager Privacy Statement on-line, go to https://go.microsoft.com/fwlink/?LinkID=626527.

Setup Downloader for System Center Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Before you run Setup to install or upgrade a System Center Configuration Manager site, you can use the Setup Downloader standalone application from the version of Configuration Manager that you want to install to download updated Setup files.

Using updated Setup files ensures that your site installation uses current versions of key installation files. In oveview:

- When you use Setup Downloader to download files prior to starting setup, you specify a folder to contain the files.
- The account you use to run Setup Downloader must have **Full Control** permissions to the download folder.
- When you run Setup to install or upgrade a site, you can direct it to use this local copy of files you previously downloaded. This prevents Setup form having to connect to Microsoft when you start the site install or upgrade.
- You can use the same local copy of setup files for subsequent site installations or upgrades.

The following types of files are downloaded by Setup Downloader:

- Required prerequisite redistributable files
- Language packs
- The latest product updates for Setup

You have two options for running Setup Downloader:

- Run the application with the user interface
- For command-line options, run the application at a command prompt

Run Setup Downloader with the user interface

1. On a computer that has Internet access, open Windows Explorer, and go to **<ConfigMgrInstallationMedia>\SMSSETUP\BIN\X64**.
2. To open Setup Downloader, double-click **Setupdl.exe**.
3. Specify the path for the folder that will host the updated installation files, and then click **Download**. Setup Downloader verifies the files that are currently in the download folder. It downloads only files that are missing or that are newer than existing files. Setup Downloader creates subfolders for downloaded languages, and other required subfolders.
4. To review the download results, open the **ConfigMgrSetup.log** file in the root directory of drive C. .

Run Setup Downloader from a command prompt

1. In a Command Prompt window, go to **<*Configuration Manager installation media*>\SMSSETUP\BIN\X64**.
2. To open Setup Downloader, run **Setupdl.exe**.

You can use the following command-line options with **Setupdl.exe**:

- **/VERIFY**: Use this option to verify the files in the download folder, which include language files. Review the ConfigMgrSetup.log file in the root directory of drive C for a list of files that are outdated. No files are downloaded when you use this option.
- **/VERIFYLANG**: Use this option to verify the language files in the download folder. Review the ConfigMgrSetup.log file in the root directory of drive C for a list of language files that are outdated.
- **/LANG**: Use this option to download only the language files to the download folder.
- **/NOUI**: Use this option to start Setup Downloader without displaying the user interface. When you use this option, you must specify the **download path** as part of the command at the command prompt.
- **<DownloadPath>**: You can specify the path to the download folder to automatically start the verification or download process. You must specify the download path when you use the **/NOUI** option. If you do not specify a download path, you must specify the path when Setup Downloader opens. Setup Downloader creates the folder if it does not exist.

Example commands:

- **setupdl <DownloadPath>**
  - Setup Downloader starts, verifies the files in the specified download folder, and then downloads only the files that are missing or that have newer versions than existing files.
- **setupdl /VERIFY <DownloadPath>**
  - Setup Downloader starts and verifies the files in the specified download folder.
- **setupdl /NOUI <DownloadPath>**
  - Setup Downloader starts, verifies the files in the specified download folder, and then downloads only the files that are missing or that are newer than the existing files.
- **setupdl /LANG <DownloadPath>**
  - Setup Downloader starts, verifies the language files in the specified download folder, and then downloads only the language files that are missing or that are newer than the existing files.
- **setupdl /VERIFY**
  - Setup Downloader starts, and then you must specify the path to the download folder. Next, after you click **Verify**, Setup Downloader verifies the files in the download folder.

3. To review the download results, open the **ConfigMgrSetup.log** file in the root directory of drive C.

Prerequisite Checker for System Center Configuration Manager

9/11/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Before you run Setup to install or upgrade a System Center Configuration Manager site, or before you install a site system role on a new server, you can use this stand-alone application (**Prereqchk.exe**) from the version of Configuration Manager that you want use to verify server readiness. Use Prerequisite Checker to identify and fix problems that would block a site or site system role installation.

> **NOTE**
> Prerequisite Checker always runs as part of Setup.

By default, when Prerequisite Checker runs:

- It validates the server where it runs.
- The local computer is scanned for an existing site server, and only the checks that are applicable to the site are run.
- If no existing sites are detected, all prerequisite rules are run.
- It checks rules to verify that software and settings required for setup are installed. It's possible that required software will require additional configuration or software updates that are not verified by Prerequisite Checker.
- It logs its results in the **ConfigMgrPrereq.log** file on the system drive of the computer. The log file might contain additional information that doesn't appear in the application interface.

When you run Prerequisite Checker at a command prompt and specify specific command-line options:

- Prerequisite Checker performs only the checks that are associated with the site server or site systems that you specify in the command line.
- To check a remote computer, your user account must have Administrator rights to the remote computer.

For more information about the checks that Prerequisite Checker performs, see List of prerequisite checks for System Center Configuration Manager.

Copy Prerequisite Checker files to another computer

1. In Windows Explorer, go to one of the following locations:
   - **<*Configuration Manager installation media*>\SMSSETUP\BIN\X64**
   - **<*Configuration Manager installation path*>\BIN\X64**
2. Copy the following files to the destination folder on the other computer:
   - Prereqchk.exe
   - Prereqcore.dll
   - Basesql.dll
   - Basesvr.dll
   - Baseutil.dll

Run Prerequisite Checker with default checks

1. In Windows Explorer, go to one of the following locations:

   - **<*Configuration Manager installation media*>\SMSSETUP\BIN\X64**
   - **<*Configuration Manager installation path*>\BIN\X64**
2. Run **prereqchk.exe** to start Prerequisite Checker.
   Prerequisite Checker detects existing sites, and if found, performs checks for upgrade readiness. If no sites are found, all checks are performed. The **Site Type** column provides information about the site server or site system with which the rule is associated.

Run Prerequisite Checker from a command prompt for all default checks

1. Open a Command Prompt window and change directories to one of the following locations:

   - **<*Configuration Manager installation media*>\SMSSETUP\BIN\X64**
   - **<*Configuration Manager installation path*>\BIN\X64**
2. Enter **prereqchk.exe /LOCAL** to start Prerequisite Checker and run all prerequisite checks on the server.

Run Prerequisite Checker from a command prompt to use options

1. Open a Command Prompt window and change directories to one of the following locations:

   - **<*Configuration Manager installation media*>\SMSSETUP\BIN\X64**
   - **<*Configuration Manager installation path*>\BIN\X64**
2. Enter **prereqchk.exe** with the addition of one or more of the following command-line options.

   For example, to check a primary site, you might use the following:

   prereqchk.exe [/NOUI] /PRI /SQL <FQDN of SQL Server> /SDK <FQDN of SMS Provider> [/JOIN <FQDN of central administration site>] [/MP <FQDN of management point>] [/DP <FQDN of distribution point>]

   Central administration site server:

   - **/NOUI**

     Not required. Starts Prerequisite Checker without displaying the user interface. You must specify this option before any other option in the command line.

   - **/CAS**

     Required. Verifies that the local computer meets the requirements for the central administration site.

   - **/SQL <*FQDN of SQL Server*>**

     Required. Using the fully qualified domain name (FQDN), verifies that the specified computer meets the requirements for SQL Server to host the Configuration Manager site database.

   - **/SDK <*FQDN of SMS Provider*>**

     Required. Verifies that the specified computer meets the requirements for the SMS Provider.

   - **/Ssbport**

     Not required. Verifies that a firewall exception is in effect to allow communication on the SQL Server Service Broker (SSB) port. The default SSB port is 4022.

- **InstallDir <*Configuration Manager installation path*>**

  Not required. Verifies the minimum disk space on requirements for site installation.

Primary site server:

- **/NOUI**

  Not required. Starts Prerequisite Checker without displaying the user interface. You must specify this option before any other option in the command line.

- **/PRI**

  Required. Verifies that the local computer meets the requirements for the primary site.

- **/SQL <*FQDN of SQL Server*>**

  Required. Verifies that the specified computer meets the requirements for SQL Server to host the Configuration Manager site database.

- **/SDK <*FQDN of SMS Provider*>**

  Required. Verifies that the specified computer meets the requirements for the SMS Provider.

- **/JOIN <*FQDN of central administration site*>**

  Not required. Verifies that the local computer meets the requirements for connecting to the central administration site server.

- **/MP <*FQDN of management point*>**

  Not required. Verifies that the specified computer meets the requirements for the management point site system role. This option is only supported when you use the **/PRI** option.

- **/DP <*FQDN of distribution point*>**

  Not required. Verifies that the specified computer meets the requirements for the distribution point site system role. This option is only supported when you use the **/PRI** option.

- **/Ssbport**

  Not required. Verifies that a firewall exception is in effect to allow communication on the SSB port. The default SSB port is 4022.

- **InstallDir <*Configuration Manager installation path*>**

  Not required. Verifies the minimum disk space on requirements for site installation.

Secondary site server:

- **/NOUI**

  Not required. Starts Prerequisite Checker without displaying the user interface. You must specify this option before any other option in the command line.

- **/SEC <*FQDN of secondary site server*>**

  Required. Verifies that the specified computer meets the requirements for the secondary site.

- **/INSTALLSQLEXPRESS**

  Not required. Verifies that SQL Server Express can be installed on the specified computer.

- **/Ssbport**

Not required. Verifies that a firewall exception is in effect to allow communication for the SSB port. The default SSB port is 4022.

- **/Sqlport**

  Not required. Verifies that a firewall exception is in effect to allow communication for the SQL Server service port, and that the port is not in use by another named instance of SQL Server. The default port is 1433.

- **InstallDir <*Configuration Manager installation path*>**

  Not required. Verifies the minimum disk space on requirements for site installation.

- **/SourceDir**

  Not required. Verifies that the computer account of the secondary site can access the folder that hosts the source files for Setup.

Configuration Manager console:

- **/Adminui**

  Required. Verifies that the local computer meets the requirements for installing Configuration Manager.

3. In the Prerequisite Checker user interface, Prerequisite Checker creates a list of discovered problems in the **Prerequisite result** section.

   - Click an item in the list for details about how to resolve the problem.
   - You must resolve all items in the list that have an **Error** status before you install the site server, site system, or the Configuration Manager console.
   - You also can open the **ConfigMgrPrereq.log** file in the root of the system drive to review Prerequisite Checker results. The log file might contain additional information that is not displayed in the Prerequisite Checker user interface.

List of prerequisite checks for Configuration Manager

7/26/2019 • 22 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article details the prerequisite checks that run when you install or update Configuration Manager. For more information, see Prerequisite checker.

Errors

Active migration mappings on the target primary site

Applies to: Central administration site

There are no active migration mappings to primary sites.

Active replica MP

Applies to: Primary site

There's an active management point replica.

Administrative rights on expand primary site

Applies to: Central administration site

When you expand a primary site to a hierarchy, the user account that runs setup has **Administrator** rights on the standalone primary site server.

Administrative rights on site system

Applies to: Central administration site, primary site, secondary site

The user account that runs Configuration Manager setup has **Administrator** rights on the site server.

Administrator rights on central administration site

Applies to: Primary site

The user account that runs Configuration Manager setup has **Administrator** rights on the central administration site server.

Asset Intelligence synchronization point on the expanded primary site

Applies to: Central administration site

When you expand a primary site to a hierarchy, the Asset Intelligence synchronization point role isn't installed on the standalone primary site.

BITS enabled

Applies to: Management point

Background Intelligent Transfer Service (BITS) is installed on the management point. This check can fail for one of the following reasons:

- BITS isn't installed
- The IIS 6.0 WMI compatibility component for IIS 7.0 isn't installed on the server or remote IIS host
- Setup was unable to verify remote IIS settings. IIS common components aren't installed on the site server.

Case-insensitive collation on SQL Server

Applies to: Site database server

The SQL Server installation uses a case-insensitive collation, such as **SQL_Latin1_General_CP1_CI_AS**.

Central administration site server administrative rights on expand primary site

Applies to: Central administration site

When you expand a primary site to a hierarchy, the computer account of the central administration site server has **Administrator** rights on the standalone primary site server.

Client version on management point computer

Applies to: Management point

You're installing the management point on a server that doesn't have a different version of the Configuration Manager client installed.

Cloud management gateway on the expanded primary site

Applies to: Central administration site

When you expand a primary site to a hierarchy, the cloud management gateway role isn't installed on the standalone primary site.

Connection to SQL Server on central administration site

Applies to: Primary site

The user account that runs Configuration Manager setup on the primary site to join an existing hierarchy has the **sysadmin** role on the SQL Server instance for the central administration site.

Custom client agent settings have NAP enabled

Applies to: Central administration site, primary site

There are no custom client settings that enable network access protection (NAP).

Data warehouse service point on the expanded primary site

Applies to: Central administration site

When you expand a primary site to a hierarchy, the data warehouse service point role isn't installed on the standalone primary site.

Dedicated SQL Server instance

Applies to: Central administration site, primary site, secondary site

You configured a dedicated instance of SQL Server to host the Configuration Manager site database.

If another site uses the instance, you must select a different instance for the new site. You can also uninstall the other site, or move its database to a different instance for the SQL server.

Default client agent settings have NAP enabled

Applies to: Central administration site, primary site

The default client settings don't enable network access protection (NAP).

Domain membership (error)

Applies to: Central administration site, primary site, secondary site, SMS Provider, SQL Server

The Configuration Manager computer is a member of a Windows domain.

Endpoint Protection point on the expanded primary site

Applies to: Central administration site

When you expand a primary site to a hierarchy, the Endpoint Protection point role isn't installed on the standalone primary site.

Existing Configuration Manager server components on server

Applies to: Central administration site, primary site, secondary site

A site server or site system role isn't already installed on the server selected for site installation.

Existing stand-alone primary site for version and site code

Applies to: Central administration site, primary site

The primary site you plan to expand is a standalone primary site. It has the same version of Configuration Manager, but a different site code than the central administration site to be installed.

Firewall exception for SQL Server

Applies to: Central administration site, primary site, secondary site, management point

The Windows Firewall is disabled or a relevant Windows Firewall exception exists for SQL Server.

Allow Sqlservr.exe or the required TCP ports to be accessed remotely. By default, SQL Server listens on TCP port 1433, and the SQL Server Service Broker (SSB) uses TCP port 4022.

Free disk space on site server

Applies to: Central administration site, primary site, secondary site

To install the site server, it must have at least 15 GB of free disk space. If you install the SMS Provider on the same server, it needs an additional 1 GB of free space.

IIS service running

Applies to: Management point, distribution point

IIS is installed and running on the server for the management point or distribution point.

Incompatible collection references

Applies to: Central administration site

During an upgrade, collections reference only other collections of the same type.

Match collation of expand primary site

Applies to: Central administration site

When you expand a primary site to a hierarchy, the site database for the standalone primary site has the same collation as the site database at the central administration site.

Maximum text replication size for SQL Server Always On availability groups

Applies to: Site database server

When using SQL Server Always On, the **max text repl size** setting must be properly configured. For more information, see Prepare to use SQL Server Always On availability groups with Configuration Manager.

Microsoft Intune Connector on the expanded primary site

Applies to: Central administration site

When you expand a primary site to a hierarchy, the Microsoft Intune Connector role isn't installed on the standalone primary site.

Microsoft Remote Differential Compression (RDC) library registered

Applies to: Central administration site, primary site, secondary site

The RDC library is registered on the Configuration Manager site server.

Microsoft Windows Installer

Applies to: Central administration site, primary site, secondary site

Verifies the Windows Installer version.

When this check fails, setup wasn't able to verify the version, or the installed version doesn't meet the minimum requirement of Windows Installer 4.5.

Minimum .NET Framework version for Configuration Manager console

Applies to: Configuration Manager console

Microsoft .NET Framework 4.0 is installed on the Configuration Manager console computer.

Minimum .NET Framework version for Configuration Manager site server

Applies to: Central administration site, primary site, secondary site

.NET Framework 3.5 is installed or enabled on the Configuration Manager site server.

Minimum .NET Framework version for SQL Server Express edition installation for Configuration Manager secondary site

Applies to: Secondary site

.NET Framework 4.0 is installed or enabled on the Configuration Manager secondary site server. This version is required by SQL Server Express.

Parent database collation

Applies to: Primary site, secondary site

The collation of the site database matches the collation of the parent site's database. All sites in a hierarchy must use the same database collation.

Parent site replication status

Applies to: Central administration site, primary site

The replication status of the parent site is **Replication active** (state **125**).

Pending system restart

Applies to: Central administration site, primary site, secondary site

Before you run setup, another program requires the server to be restarted.

Starting in version 1810, this check is more resilient. To see if the computer is in a pending restart state, it checks the following registry locations:

- `HKLM:Software\Microsoft\Windows\CurrentVersion\Component Based Servicing\RebootPending`
- `HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\RebootRequired`
- `HKLM:SYSTEM\CurrentControlSet\Control\Session Manager, PendingFileRenameOperations`
- `HKLM:Software\Microsoft\ServerManager, CurrentRebootAttempts`

Primary FQDN

Applies to: Central administration site, primary site, secondary site, site database server

The NetBIOS name of the computer matches the local hostname in the fully qualified domain name (FQDN).

Read-only domain controller

Applies to: Central administration site, primary site, secondary site

Site database servers and secondary site servers aren't supported on a read-only domain controller (RODC).

For more information, see the Microsoft Support article on Problems when installing SQL Server on a domain controller.

Required SQL Server collation

Applies to: Central administration site, primary site, secondary site

The instance for SQL Server is configured to use the **SQL_Latin1_General_CP1_CI_AS** collation.

If the Configuration Manager site database is already installed, this check also applies to the database. For information about changing your SQL Server instance and database collations, see SQL collation and unicode support.

If you're using a Chinese OS and require GB18030 support, this check doesn't apply. For more information about enabling GB18030 support, see International support.

Server service is running

Applies to: Central administration site, primary site, secondary site

The Server service is started and running.

Setup source folder

Applies to: Secondary site

The computer account for the secondary site has the following permissions to the setup source folder and share:

- **Read** NTFS file system permissions
- **Read** share permissions

> **NOTE**
> If you use administrative shares, for example, C$ and D$, the secondary site computer account must be an **Administrator** on the server.

Setup source version

Applies to: Secondary site

The Configuration Manager version in the specified source folder for the secondary site installation matches the Configuration Manager version of the primary site.

Site code in use

Applies to: Primary site

The specified site code isn't already in use in the Configuration Manager hierarchy. Specify a unique site code for this site.

Site server computer account administrative rights

Applies to: Primary site, site database server

The site server computer account has **Administrator** rights on the SQL server and management point.

Site server FQDN length

Applies to: Central administration site, primary site, secondary site

The length of the FQDN of the site server.

Site server in passive mode on the expanded primary site

Applies to: Central administration site

When you expand a primary site to a hierarchy, the site server in passive mode role isn't installed on the standalone primary site.

SMS Provider in same domain as site server

Applies to: SMS Provider

Any instance of the SMS Provider is in the same domain as the site server.

Software update point in NLB configuration

Applies to: Software update point

The site isn't using network load balancing (NLB) with any virtual locations for active software update points.

Software update point using a load balancer

Applies to: Software update point

Configuration Manager doesn't support software update points on network (NLB) or hardware load balancers (HLB).

SQL Server Always On availability groups

Applies to: Site database server

When using SQL Server Always On, it must meet the minimum requirements to host an availability group. For more information, see Prepare to use SQL Server Always On availability groups with Configuration Manager.

SQL Server availability group configured for readable secondaries

Applies to: Site database server

When using SQL Server Always On, check the secondary read state of availability group replicas.

SQL Server availability group configured for manual failover

Applies to: Site database server

When using SQL Server Always On, availability group replicas are configured for manual failover.

SQL Server availability group replicas on default instance

Applies to: Site database server

When using SQL Server Always On, availability group replicas are on the default instance.

SQL availability group replicas must all have the same seeding mode

Applies to: Site database server

Starting in version 1906, when using SQL Server Always On, you need to configure availability group replicas with the same seeding mode.

SQL availability group replicas must be healthy

Applies to: Site database server

Starting in version 1906, when using SQL Server Always On, availability group replicas are in a healthy state.

SQL Server configuration for site upgrade

Applies to: Site database server

The SQL Server meets the minimum requirements for site upgrade. For more information, see Supported SQL Server versions.

SQL Server edition

Applies to: Site database server

SQL Server at the site isn't SQL Server Express.

SQL Server Express on secondary site

Applies to: Secondary site

SQL Server Express can successfully install on the secondary site server.

SQL Server on the secondary site server

Applies to: Secondary site

SQL Server is installed on the secondary site server. You can't install SQL Server on a remote site system for a secondary site.

> **WARNING**
> This check only applies when you select to have setup use an existing instance of SQL Server.

SQL Server service running account

Applies to: Central administration site, primary site, secondary site

The sign-in account for the SQL Server service isn't a local user account or **LOCAL SERVICE**.

Configure the SQL Server service to use a valid domain account, **NETWORK SERVICE**, or **LOCAL SYSTEM**.

SQL Server site database consistency

Applies to: Site database server

Verify database consistency.

SQL Server sysadmin rights

Applies to: Site database server

The user account that runs Configuration Manager setup has the **sysadmin** role on the SQL Server instance that you selected for site database installation. This check also fails when setup is unable to access the instance for the SQL Server to verify permissions.

SQL Server sysadmin rights for reference site

Applies to: Site database server

The user account that runs Configuration Manager setup has the **sysadmin** role on the SQL Server role instance that you selected as the reference site database. SQL Server **sysadmin** role permissions are required to modify the site database.

SQL Server TCP port

Applies to: Site database server

TCP is enabled for the SQL Server instance, and is set to use a static port.

SQL Server version

Applies to: Site database server

A supported version of SQL Server is installed on the specified site database server.

For more information, see Support for SQL Server versions.

Unsupported OS for Configuration Manager console

Applies to: Configuration Manager console

Install the Configuration Manager console on computers that run a supported OS version.

For more information, see the Supported OS versions for the Configuration Manager console.

Unsupported OS for site server

Applies to: Central administration site, primary site, secondary site, Configuration Manager console, management point, distribution point

The server runs a supported OS version.

For more information, see Supported OS versions for Configuration Manager site system servers.

Unsupported site system role: out of band service point

Applies to: Primary site

The out of band service point site system role isn't installed.

Unsupported site system role: system health validation point

Applies to: Primary site

The system health validation point site system role isn't installed.

Unsupported upgrade path

Applies to: Central administration site, primary site

All site servers in the hierarchy meet the Configuration Manager minimum version that's required for upgrade.

USMT installed

Applies to: Central administration site, primary site (standalone only)

The User State Migration Tool (USMT) component of the Windows Assessment and Deployment Kit (ADK) for Windows is installed.

Validate FQDN of SQL Server

Applies to: Site database server

You specified a valid FQDN for the SQL Server computer.

Verify central administration site version

Applies to: Primary site

The central administration site has the same version of Configuration Manager.

Verify database consistency

Applies to: Central administration site, primary site

Verifies consistency of the site database in SQL Server.

Windows Deployment Tools installed

Applies to: SMS Provider

The Windows Deployment Tools component of the Windows ADK is installed.

Windows Failover Cluster

Applies to: Site server, management point, distribution point

Server with the site server, management point, or distribution point roles aren't part of a Windows Cluster.

Starting in version 1810, the Configuration Manager setup process no longer blocks installation of the site server role on a computer with the Windows role for Failover Clustering. SQL Always On requires this role, so previously you couldn't colocate the site database on the site server. With this change, you can create a highly available site with fewer servers by using SQL Always On and a site server in passive mode. For more information, see High availability options.

Windows PE installed

Applies to: SMS Provider

The Windows Preinstallation Environment (PE) component of the Windows ADK is installed.

Warnings

Active Directory domain functional level

Applies to: Central administration site, primary site

The Active Directory domain functional level is a minimum of Windows Server 2008 R2.

Administrative rights on distribution point

Applies to: Distribution point

The user account running setup has **Administrator** rights on the distribution point.

Administrative rights on management point

Applies to: Management point, distribution point

The computer account of the site server has **Administrator** rights on the management point and distribution point.

Administrative share (site system)

Applies to: Management point

The required administrative shares are present on the site system computer.

Application compatibility

Applies to: Central administration site, primary site

Current applications are compliant with the application schema.

Backlogged inboxes

Applies to: Central administration site, primary site

The site server is processing critical inboxes in a timely fashion. Inboxes don't contain files older than one day.

It checks the following inbox folders:

- `despoolr.box\receive\*.i??`
- `despoolr.box\receive\*.s??`
- `despoolr.box\receive\*.nil`
- `schedule.box\requests\*.sr?`

To resolve this warning, check whether the despooler and scheduler site system components are running.

BITS installed

Applies to: Management point

The Background Intelligent Transfer Service (BITS) is installed and enabled in IIS.

Cloud management gateway requires either token-based authentication or an HTTPS management point

Applies to: Cloud management gateway

With some versions of Configuration Manager, you can't use an HTTP management point with the cloud management gateway (CMG). Either configure the CMG for HTTPS, or configure the site for enhanced HTTP. For more information, see Plan for cloud management gateway.

Configuration for SQL Server memory usage

Applies to: Site database server

SQL Server is configured for unlimited memory use. Configure SQL Server memory to have a maximum limit.

Distribution point package version

Applies to: Distribution points

All distribution points in the site have the latest version of software distribution packages.

Domain membership (warning)

Applies to: Management point, distribution point

The Configuration Manager computer is a member of a Windows domain.

Firewall exception for SQL Server (standalone primary site)

Applies to: Primary site (standalone only)

The Windows Firewall is disabled, or a relevant Windows Firewall exception exists for SQL Server.

Allow Sqlservr.exe or the required TCP ports to be accessed remotely. By default, SQL Server listens on TCP port 1433, and the Server Service Broker (SSB) uses TCP port 4022.

Firewall exception for SQL Server for management point

Applies to: Management point

The Windows Firewall is disabled, or a relevant Windows Firewall exception exists for SQL Server.

IIS HTTPS configuration

Applies to: Management point, distribution point

IIS website has bindings for the HTTPS communication protocol.

When you install site roles that require HTTPS, configure IIS site bindings on the specified server with a valid public key infrastructure (PKI) certificate.

Microsoft XML Core Services 6.0 (MSXML60)

Applies to Central administration site, primary site, secondary site, Configuration Manager console, management point, distribution point

Verifies that MSXML 6.0 or a later version is installed.

Network access protection (NAP) is no longer supported

Applies to: Primary site

There are no software updates that are enabled for NAP.

NTFS drive on site server

Applies to: Primary site

The disk drive is formatted with the NTFS file system. For better security, install site server components on disk drives formatted with the NTFS file system.

Pending configuration item policy updates

Applies to: Primary site

Starting in version 1806, if you're updating from version 1706 or later, you may see this warning if you have many application deployments and at least one of them requires approval.

You have two options:

- Ignore the warning and continue with the update. This action causes higher processing on the site server during the update as it processes the policies. You may also see more processor load on the management point after the update.
- Revise one of the applications that has no requirements or a specific OS requirement. Pre-process some of the load on the site server at that time. Review **objreplmgr.log**, and then monitor the processor on the management point. After the processing is complete, update the site. There will still be some additional processing after the update, but less than if you ignore the warning with the first option.

Pending system restart on the remote SQL Server

Applies to: Version 1902 and later, remote SQL Server

Before you run setup, another program requires the server to be restarted.

To see if the computer is in a pending restart state, it checks the following registry locations:

- `HKLM:Software\Microsoft\Windows\CurrentVersion\Component Based Servicing\RebootPending`
- `HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\RebootRequired`
- `HKLM:SYSTEM\CurrentControlSet\Control\Session Manager, PendingFileRenameOperations`
- `HKLM:Software\Microsoft\ServerManager, CurrentRebootAttempts`

PowerShell 2.0 on site server

Applies to: Primary site with Exchange connector

Windows PowerShell 2.0 or a later version is installed on the site server for the Configuration Manager Exchange Connector.

Remote connection to WMI on secondary site

Applies to: Secondary site

Setup can establish a remote connection to WMI on the secondary site server.

Schema extensions

Applies to: Central administration site, primary site

The Active Directory schema has been extended. If it's extended, the version of the schema extensions that were used.

Configuration Manager doesn't require Active Directory schema extensions for site server installation. Microsoft recommends them for the full use of all Configuration Manager features. For more information about the advantages of extending the schema, see Prepare Active Directory for site publishing.

Share name in package

Applies to: Central administration site, primary site

Packages don't have invalid characters in the share name, such as `#`.

Site system to SQL Server communication

Applies to: Secondary site, management point

The account that you configured to run the SQL Server service for the site database instance has a valid service principal name (SPN) in Active Directory Domain Services. Register a valid SPN in Active Directory to support Kerberos authentication.

SQL Server change tracking cleanup

Applies to: Site database server

Starting in version 1810, check if the site database has a backlog of SQL change tracking data.

Manually verify this check by running a diagnostic stored procedure in the site database. First, create a diagnostic connection to your site database. The easiest method is to use SQL Server Management Studio's Database Engine Query Editor, and connect to `admin:<instance name>`.

In a dedicated administrator connection query window, run the following commands:

```
USE <ConfigMgr database name>
EXEC spDiagChangeTracking
```

Depending upon the size of your database and the backlog size, this stored procedure could run in a few minutes or several hours. When the query completes, you see two sections of data related to the backlog. First look at **CT_Days_Old**. This value tells you the age (days) of the oldest entry in your syscommittab table. It should be five days, which is the Configuration Manager default value. Don't change this default value. At times of heavy data processing or replication, the oldest entry in syscommittab could be over five days. If this value is above seven days, run a manual cleanup of change tracking data.

To clean up the change tracking data, run the following command in the dedicated administration connection:

```
USE <ConfigMgr database name>
EXEC spDiagChangeTracking @CleanupChangeTracking = 1
```

This command starts a cleanup of syscommittab and all of the associated side tables. It can run in several minutes or several hours. To monitor its progress, query the **vLogs** view. To see the current progress, run the following query:

```
SELECT * FROM vLogs WHERE ProcedureName = 'spDiagChangeTracking'
```

SQL Server Native Client

When you install a new site, Configuration Manager automatically installs SQL Server Native Client as a redistributable component. After the site is installed, Configuration Manager doesn't upgrade SQL Server Native Client. Updating the SQL Server Native Client may require a restart, which can impact the site install process.

This check makes sure the site has a supported version of the SQL Native Client. Starting in version 1810, the minimum version is SQL 2012 SP4 (`11.*.7001.0`).

This SQL Native Client version supports TLS 1.2. For more information, see the following articles:

- TLS 1.2 support for Microsoft SQL Server
- How to enable TLS 1.2 for Configuration Manager

Configuration Manager uses SQL Server Native Client on the following site system roles:

- Site database server

- Site server: central administration site, primary site, or secondary site
- Management point
- Device management point
- State migration point
- SMS Provider
- Software update point
- Multicast-enabled distribution point
- Asset Intelligence update service point
- Reporting services point
- Application catalog web service
- Enrollment point
- Endpoint Protection point
- Service connection point
- Certificate registration point
- Data warehouse service point

SQL Server process memory allocation

Applies to: Site database server

SQL Server reserves a minimum of 8 GB of memory for the central administration site and primary site, and a minimum of 4 GB of memory for the secondary site.

For more information, see How to configure memory options using SQL Server Management Studio.

> **NOTE**
> This check isn't applicable to SQL Server Express on a secondary site. This edition is limited to 1 GB of reserved memory.

SQL Server security mode

Applies to: Site database server

SQL Server is configured for Windows authentication security.

Unsupported site system OS version for upgrade

Applies to: Primary site, secondary site

Site system roles other than distribution points are installed on servers running Windows Server 2012 or later.

For more information, see Supported operating systems for Configuration Manager site system servers.

> **NOTE**
> This check can't resolve the status of site system roles installed in Azure or for the cloud storage used by Microsoft Intune. Ignore warnings for these roles as false positives.

Upgrade Assessment Toolkit is unsupported

Applies to: Central administration site, primary site

The Upgrade Assessment Toolkit isn't installed. For more information, see Removed and deprecated features.

Verify site server permissions to publish to Active Directory

Applies to: Central administration site, primary site, secondary site

The computer account for the site server has **Full Control** permissions to the **System Management** container in

the Active Directory domain.

For more information, see Prepare Active Directory for site publishing.

> **NOTE**
>
> If you manually verify the permissions, you can ignore this warning.

Windows Remote Management (WinRM) v1.1

Applies to: Primary site, Configuration Manager console

WinRM 1.1 is installed on the primary site server or the Configuration Manager console computer to run the out-of-band management console.

For more information about how to download WinRM 1.1, see Support article 936059.

WSUS on site server

Applies to: Central administration site, primary site

A supported version of Windows Server Update Services (WSUS) is installed on the site server.

When you use a software update point on a server other than the site server, you must install the WSUS Administration Console on the site server. For more information about WSUS, see Windows Server Update Services.

Resources for installing System Center Configuration Manager sites

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The following topics can help you install System Center Configuration Manager or add sites to your existing Configuration Manager hierarchy.

- Prepare to install sites

  This topic offers essential information that can help you install a site to a new or existing hierarchy. Information includes when to choose non-default source files, limitations that apply to all sites, and optional actions you can take to help simplify your tasks when you install more than one site.

- Prerequisites for installing sites

  Learn about the user rights and permissions your account must have to install a site and related prerequisites for each type of site you can install.

- Install sites using the Setup Wizard

  This topic walks you through the site installation wizard. It provides details about options that might not be clear in the wizard user interface.

- Install sites using a command line and script

  Learn how to get a site installation script, and how to use it for unattended site installs.

- Install the Configuration Manager console

  This topic has guidance on how to install the Configuration Manager console on a computer on which you are not installing a site.

- Upgrade an evaluation installation to a full installation

  Read this topic when you're ready to upgrade your evaluation site to a fully licensed Configuration Manager site.

Prepare to install System Center Configuration Manager sites

9/11/2019 • 7 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To prepare for a successful deployment of one or more System Center Configuration Manager sites, become familiar with the details in this article. These steps can save you time during installation of multiple sites and help prevent missteps that might result in the need to reinstall one or more sites.

> **TIP**
> When managing System Center Configuration Manager site and hierarchy infrastructure, the terms *upgrade*, *update*, and *install* are used to describe three separate concepts. To learn how each term is used, see About upgrade, update, and install.

Options for installing different types of sites

When you install a new Configuration Manager site, the version of the source files that you can use depends on the version of sites that are already in the hierarchy (if any). The installation methods that you can use depend on the type of site you want to install.

Before installing a site, make sure you have planned your hierarchy, and that you understand the type of site you want to install. For more information, see Design a hierarchy of sites.

First site

The first site that you install in a hierarchy will be either a stand-alone primary site or a central administration site.

Installation media: To install a central administration site or a stand-alone primary site as the first site in a new hierarchy, you must use a baseline version of Configuration Manager. Do not install the first site of a new hierarchy by using updated source files from the CD.Latest folder of any site.

Installation method: You can install either type of site by using the Configuration Manager Setup Wizard, or you can configure a script to use with a scripted command-line installation.

Additional sites

After the initial site is installed, you can add more sites at any time. You have the following options for adding sites (up to supported limits):

SITE THAT YOU HAVE	ADDITIONAL SITE TYPE YOU CAN INSTALL
Central administration site	Child primary site
Child primary site	Secondary site
Stand-alone primary site	Secondary site (you can expand the primary site, which converts the stand-alone primary site to a child primary site)

Installation media: When you install a central administration site to expand a stand-alone primary site, or if you install a new child primary site in an existing hierarchy, you must use installation media (that contains source files) that matches the version of the existing site or sites.

> **IMPORTANT**
> If you have installed in-console updates that have changed the version of the previously installed sites, do not use the original installation media. Instead, in that scenario, use source files from the CD.Latest folder of an updated site. Configuration Manager requires you to use source files that match the version of the existing site that your new site will connect to.

A secondary site must be installed from the Configuration Manager console. This way, secondary sites are always installed by using source files from the parent primary site.

Installation method: The method you use to install additional sites depends on the type of site you want to install.

- **Add a central administration site**: You can use the Configuration Manager Setup Wizard or a scripted command line to install the new central administration site as a parent site to your existing stand-alone primary site. For more information, see Expanding a stand-alone primary site.
- **Add a child primary site**: You can use the Configuration Manager Setup Wizard or a command-line installation to add a child primary site below a central administration site.
- **Add a secondary site**: Use the Configuration Manager console to install a secondary site as a child site below a primary site. Other methods are not supported for adding secondary sites.

Common tasks to complete before starting an installation

- **Understand the hierarchy topology you will use for your deployment**
  For more information, see Design a hierarchy of sites for System Center Configuration Manager.
- **Prepare and configure individual servers to meet prerequisites and supported configurations for use with Configuration Manager**
  For more information, see Site and site system prerequisites.
- **Install and configure SQL Server to host the site database**
  For more information, see Support for SQL Server versions for System Center Configuration Manager.
- **Prepare your network environment to support Configuration Manager**
  For more information, see Configure firewalls, ports, and domains to prepare for Configuration Manager.
- **If you will use a public key infrastructure (PKI), prepare your infrastructure and certificates**
  For more information, see PKI certificate requirements for Configuration Manager.
- **Install the latest security updates on computers you will use as site servers or site system servers, and when necessary, restart them**

About site names and site codes

Site codes and site names are used to identify and manage the sites in a Configuration Manager hierarchy. In the Configuration Manager console, the site code and site name are displayed in the *<site code> - <site name>* format. Every site code that you use in your hierarchy must be unique. If the Active Directory schema is extended for Configuration Manager and your sites are publishing data, the site codes used within an Active Directory forest must be unique even if they are used in a different Configuration Manager hierarchy or if they have been used in earlier Configuration Manager installations. Be sure to carefully plan your site codes and site names before you deploy your hierarchy.

Specify a site code and site name

When you run Configuration Manager Setup, you are prompted for a site code and site name for the central administration site, and for each primary site and secondary site installation. A site code must uniquely identify

each site in the hierarchy. Because the site code is used in folder names, never use the following names for the site code, which include names reserved for Configuration Manager and Windows:

- AUX
- CON
- NUL
- PRN
- SMS

> **NOTE**
> Configuration Manager Setup does not verify that a site code is not already in use.

To enter the site code for a site when you're running Configuration Manager Setup, you must enter three alphanumeric characters. Only the letters *A* through *Z* and the numbers *0* through *9*, in any combination, are allowed in site codes. The sequence of letters or numbers has no effect on the communication between sites. For example, it is not necessary to name a primary site *ABC* and a secondary site *DEF*.

The site name is a friendly name identifier for the site. You can only use the characters *A* through *Z*, *a* through *z*, *0* through *9*, and the hyphen (-) in site names.

> **IMPORTANT**
> A change of the site code or site name after you install the site is not supported.

Reuse a site code

Site codes cannot be used more than one time in a Configuration Manager hierarchy for a central administration site or for a primary site, even if the original site and site code have been uninstalled. If you reuse a site code, you risk having object ID conflicts in your hierarchy. You can reuse the site code for a secondary site if that secondary site and the site code are no longer in use in your Configuration Manager hierarchy or in the Active Directory forest.

Limits and restrictions for installed sites

Before you install a site, it's important to understand the following limitations that apply to sites and site hierarchies:

- After running Setup, you cannot change the following site properties without uninstalling the site and then reinstalling it by using the new values:
  - Program Files installation directory
  - Site code
  - Site description
- When your hierarchy includes a central administration site:
  - Configuration Manager does not support moving a child primary site out of a hierarchy to create a stand-alone primary site or to attach it to a different hierarchy. Instead, uninstall the child primary site, and then reinstall it as a new stand-alone primary site or as a child site of the central administration site of a different hierarchy.

Optional steps before running Setup

Manually run Setup Downloader

To download the updated Setup files for Configuration Manager, you can run Setup Downloader. If the computer

where you will run Setup is not connected to the Internet, or if you expect to install multiple site servers, consider using Setup Downloader to download the required updates to Setup. Here's additional information:

- By default, Setup connects to the Internet to download updated Setup files.
- By default, the files are stored in the Redist folder.
- You can direct Setup to a location on your network where you have previously stored a copy of these files.

Manually run Prerequisite Checker

To identify and fix problems before you run Setup to install a site and before you install a site system role on a server, you can run Prerequisite Checker. Prerequisite Checker helps ensure that the computer meets the requirements to host the site or site system role. Here's additional information:

- By default, Setup runs Prerequisite Checker.
- If there are any errors, Setup stops until the issue is fixed.

Identify optional ports

You can identify optional ports for site systems and clients to use. Here's additional information:

- By default, site systems and clients use predefined ports to communicate.
- During Setup, you can configure alternate ports.

For more information, see Ports used in System Center Configuration Manager.

Prerequisites for installing Configuration Manager sites

8/1/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Before you begin a site installation, learn about the prerequisites for installing the different types of Configuration Manager sites.

Primary sites and the central administration site

The following prerequisites apply to installing one of the following types:

- A central administration site as the first site of a hierarchy
- A stand-alone primary site
- A child primary site

If you're installing a central administration site as part of a hierarchy expansion, see Expanding a stand-alone primary site.

Prerequisites for installing a primary site or a central administration site

- The necessary Windows Server roles, features, and Windows components must be installed. For more information, see Site system prerequisites
- The user account that installs the site must have the following rights:
  - **Administrator** on the following servers:
    - The site server
    - Each server that hosts the **site database**
    - Each instance of the **SMS Provider** for the site
  - **Sysadmin** on the instance of SQL Server that hosts the site database

    > **IMPORTANT**
    > When Configuration Manager setup finishes, the site server computer account must retain sysadmin rights to SQL Server. Don't remove the SQL sysadmin rights from this account.

- If you're installing a primary site, you need the following additional rights:
  - **Administrator** on additional servers where you install the initial management point and distribution point, if not on the site server
- If you're installing a new child primary site below a central administration site, you need the following additional rights:
  - **Administrator** on the server that hosts the central administration site
  - Role-based administration rights within Configuration Manager that are equivalent to the security role of **Infrastructure Administrator** or **Full Administrator**
- Use the correct installation source files, and run setup from that location. For information about the correct

source files to use to install different types of sites, see Options for installing different types of sites.

- The site server must have access to updated setup files from Microsoft, in one of the following ways:
  - Before you start the install, download and store a copy of these files on your local network. For more information, see Setup Downloader.
  - If a local copy of these file isn't available, the site server must have internet access. It downloads these files from Microsoft during the installation.
- The site server and site database server must meet all prerequisite configurations. Before starting Configuration Manager setup, manually run Prerequisite Checker to identify and fix problems.

Prerequisites to expand a stand-alone primary site

A stand-alone primary site must meet the following prerequisites before you can expand it into a hierarchy with a central administration site:

Source file version matches site version

Install the new central administration site using media from a CD.Latest folder that matches the version of the stand-alone primary site. To make sure the versions match, use the source files found in the CD.Latest folder on the stand-alone primary site.

For more information about the correct source files to use to install different sites, see Options for installing different types of sites.

Stop active migration from another hierarchy

You can't configure the stand-alone primary site to migrate data from another Configuration Manager hierarchy. Stop active migration to the stand-alone primary site from other Configuration Manager hierarchies and remove all configurations for migration. These configurations include:

- Migration jobs that haven't completed
- Data gathering
- The configuration of the active source hierarchy

This configuration is necessary because Configuration Manager migrates data from the top-level site of the hierarchy. When you expand a stand-alone primary site, the configurations for migration don't transfer to the central administration site.

After you expand the stand-alone primary site, if you reconfigure migration at the primary site, the central administration site performs the migration operations.

For more information about how to configure migration, see Configure source hierarchies and source sites for migration.

Computer account as Administrator

The computer account of the server that hosts the new central administration site must be a member of the **Administrator** group on the stand-alone primary site server.

To successfully expand the stand-alone primary site, the computer account of the new central administration site must have **Administrator** rights on the stand-alone primary site. This is required only during site expansion. When site expansion finishes, you can remove the account from the user group on the primary site.

Installation account permissions

The user account that runs Configuration Manager setup to install the new central administration site must have role-based administration rights at the stand-alone primary site.

To install a central administration site as part of a site expansion, the user account that runs setup to install the central administration site must be defined in role-based administration at the stand-alone primary site as either a **Full Administrator** or an **Infrastructure Administrator**.

For more information including the complete list of required permissions, see Site installation account.

Top-level site roles

Before you expand the site, uninstall the following site system roles from the stand-alone primary site:

- Asset Intelligence sync point
- Endpoint Protection point
- Service connection point

Configuration Manager only supports these roles at the top-level site of the hierarchy. Uninstall these site system roles before you expand the stand-alone primary site. After you expand the site, reinstall these site system roles at the central administration site.

All other site system roles can remain installed at the primary site.

Open the SQL Server Service Broker port

The network port must be open for the SQL Server Service Broker (SSB) between the stand-alone primary site and the server for the central administration site.

To successfully replicate data between a central administration site and a primary site, Configuration Manager requires an open port between the two sites for SSB to use. When you install a central administration site and expand a stand-alone primary site, the prerequisite check doesn't verify that the port you specify for the SSB is open on the primary site.

Known issues with Azure services

After you expand the site, you need to reconfigure the following Azure services with Configuration Manager:

- Log Analytics
- Upgrade Readiness
- Microsoft Store for Business
- Cloud management gateway

On version 1806 and later, renew the Azure Active Directory tenant secret key. For more information, seeRenew secret key.

Alternatively, remove and then recreate the connection to that service:

1. In the Configuration Manager console, delete the Azure service from the **Azure Services** node.
2. In the Azure portal, delete the tenant that's associated with the service from the Azure Active Directory tenants node. This action also deletes the Azure AD web app that's associated with the service.
3. Reconfigure the connection to the Azure service for use with Configuration Manager.

Secondary sites

The following are prerequisites for installing secondary sites:

- The necessary Windows Server roles, features, and Windows components must be installed. For more information, see Site system prerequisites
- The administrator who configures the installation of the secondary site in the Configuration Manager console must have role-based administration rights that are equivalent to the security role of **Infrastructure Administrator** or **Full Administrator**.
- The computer account of the parent primary site must be an **Administrator** on the secondary site server.
- When the secondary site uses a previously installed instance of SQL Server to host the secondary site database:

- The computer account of the parent primary site must have **sysadmin** rights on the instance of SQL Server on the secondary site server.
- The **Local System** account of the secondary site server computer must have **sysadmin** rights on the instance of SQL Server on the secondary site server.

  > **IMPORTANT**
  > When Configuration Manager setup finishes, both accounts must retain sysadmin rights to SQL Server. Don't remove the sysadmin rights from these accounts.

- The secondary site server must meet all prerequisite configurations. These configurations include SQL Server and the default site system roles of the management point and distribution point.

Next steps

After you've confirmed the prerequisites, you're ready to run setup. For more information, see Use the Setup Wizard to install Configuration Manager sites.

Use the Setup Wizard to install Configuration Manager sites

9/5/2019 • 21 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To install a new Configuration Manager site by using a guided user interface, use the Configuration Manager Setup Wizard (setup.exe). The wizard supports installing a primary site or central administration site. You also use the wizard to upgrade an evaluation installation of Configuration Manager to a fully licensed installation. When you don't want to use the wizard, you can instead use an installation script and run an unattended command-line installation.

Install a secondary site from within the Configuration Manager console. Secondary sites don't support a scripted command-line installation.

> **NOTE**
>
> Starting in version 1906, the **splash.hta** file no longer exists at the root of the installation media. It provided links to the following information:
>
> - **Install site**: `smssetup\bin\x64\setup.exe`. For more information, see Install a central administration or primary site.
> - **Before you begin**: Design a hierarchy of sites
> - **Assess server readiness**: Prerequisite Checker
> - **Download required prerequisite files**: `smssetup\bin\x64\setupdl.exe`. For more information, see Setup Downloader.
> - **Install Configuration Manager console**: `smssetup\bin\i386\consolesetup.exe`. For more information, see Install consoles.
> - **Download System Center Updates Publisher**
> - **Download clients for additional operating systems**
> - **Release notes**
> - **Read documentation**
> - **Obtain installation assistance**: TechNet Forums: Configuration Manager (Current Branch) – Site and Client Deployment
> - **Configuration Manager community**: System Center Community: How to Participate
> - **Configuration Manager home**

Install a central administration or primary site

Use the following procedure to install a central administration site or a primary site. Also use it to upgrade an evaluation site to a fully licensed Configuration Manager site.

Before starting the site installation, be familiar with the details in the following articles:

- Prepare to install sites
- Prerequisites for installing sites

If you're installing a central administration site as part of a site expansion scenario, review Expanding a stand-alone primary site before using the following procedure.

Process to install a primary or central administration site

1. On the computer where you want to install the site, run `<InstallationMedia>\SMSSETUP\BIN\X64\Setup.exe` to

start the **System Center Configuration Manager Setup Wizard**.

> **NOTE**
> When you install a central administration site to expand on a stand-alone primary site, or install a new child primary site in an existing hierarchy, use installation media (source files) that match the version of the existing site or sites. If you've installed in-console updates that have changed the version of the previously installed sites, don't use the original installation media. Instead, use source files from the CD.Latest folder of an updated site. Configuration Manager requires you to use source files that match the version of the existing site that your new site will connect to.

2. On the **Before You Begin** page, choose **Next**.
3. On the **Getting Started** page, select the type of site that you want to install:

   - **Central administration site**, as the first site of a new hierarchy, or when expanding a stand-alone primary site:

     Select **Install a Configuration Manager central administration site**.

     During a later step of this procedure, you're offered the choice to install a central administration site as the first site of a new hierarchy, or to install a central administration site to expand on a stand-alone primary site.

   - **Primary site**, as a stand-alone primary site that is the first site of a new hierarchy, or as a child primary:

     Select **Install a Configuration Manager primary site**.

     > **TIP**
     > Typically, you only select the option **Use typical installation options for a stand-alone primary site** when you want to install a stand-alone primary site in a test environment. When you select this option, setup does the following actions:
     >
     > - Automatically configures the site as a stand-alone primary site.
     > - Uses a default installation path.
     > - Uses a local installation of the default instance of SQL Server for the site database.
     > - Installs a management point and a distribution point on the site server computer.
     > - Configures the site with English and the display language of the OS on the primary site server if it matches one of the languages that Configuration Manager supports.

4. On the **Product Key** page:

   - Choose whether to install Configuration Manager as an evaluation edition or a licensed edition.
     - If you select a licensed edition, enter your product key, and choose **Next**.
     - If you select an evaluation edition, choose **Next**. (You can upgrade an evaluation installation to a full installation later.)
   - You can also specify the **Software Assurance expiration date** of your licensing agreement. It's a convenient reminder of that date. If you don't enter this date during Setup, you can specify it later from within the Configuration Manager console.

> **NOTE**
> Microsoft doesn't validate the expiration date that you entered and doesn't use this date for license validation. You can use it as a reminder of your expiration date. This date is useful because Configuration Manager periodically checks for new software updates offered online. Your software assurance license status should be current so that you're eligible to use these additional updates.

For more information, see Licensing and branches.

5. On the **Microsoft Software License Terms** page, read and accept the license terms.
6. On the **Prerequisite Licenses** page, read and accept the license terms for the prerequisite software. Setup downloads and automatically installs the software on site systems or clients when it's required. Accept all of the terms before you continue to the next page.
7. On the **Prerequisite Downloads** page, specify whether Setup must download the latest prerequisite redistributable files from the internet or use previously downloaded files:
   - If you want Setup to download the files at this time, select **Download required files**. Then specify a location to store the files.
   - If you previously downloaded the files by using Setup Downloader, select **Use previously downloaded files**. Then specify the download folder.

     > **TIP**
     > If you use previously downloaded files, verify that the path to the download folder contains the most recent version of the files.
8. On the **Server Language Selection** page, select the languages that are available for the Configuration Manager console and for reports. (English is selected by default and can't be removed.) For more information, see Language packs.
9. On the **Client Language Selection** page, select the languages that are available to client computers. Also specify whether to enable all client languages for mobile device clients. (English is selected by default and can't be removed.)

   > **IMPORTANT**
   > When you use a central administration site, make sure that client languages you configure at the central administration site include all client languages that you configure at each child primary site. Clients that install from a distribution point have access to the client languages from the top-tier site, while clients that install from a management point have access to the client languages from their assigned primary site.
10. On the **Site and Installation Settings** page, specify the following settings for the new site that you're installing:
    - **Site code**: Each site code in a hierarchy must be unique. Use three alpha-numeric digits: A through Z and 0 through 9. Because the site code is used in folder names, don't use Windows-reserved names, including:
      - AUX
      - CON
      - NUL
      - PRN

- SMS

> **NOTE**
> Setup doesn't verify whether the site code that you specify is already in use, or if it's a reserved name.

- **Site name**: Each site requires this friendly name, which can help you identify the site.
- **Installation folder**: This folder is the path to the Configuration Manager installation. You can't change the location after the site installs. The path can't contain Unicode characters or trailing spaces.

> **NOTE**
> Consider whether you want to use the default installation folder. If you use the default OS partition in a production environment, you may experience the following issues in the future:
>
> - If Configuration Manager uses the additional free disk space on the OS partition, neither Windows or Configuration Manager will operate properly. If you install Configuration Manager on a separate partition, its disk consumption won't impact the OS.
> - Configuration Manager performance is better with a fast disk. Some server designs don't optimize the OS disk for speed.
> - You can service, restore, or reinstall the OS without impacting your Configuration Manager installation.

11. On the **Site Installation** page, use the following option that matches your scenario:

    - **I'm installing a central administration site:**

      On the **Central Administration Site Installation** page, select **Install as the first site in a new hierarchy**, and then choose **Next** to continue.

    - **I'm expanding a stand-alone primary into a hierarchy with a central administration site:**

      On the **Central Administration Site Installation** page, select **Expand an existing stand-alone primary into a hierarchy**. Then specify the FQDN of the stand-alone primary site server, and choose **Next** to continue.

      The media that you use to install the new central administration site must match the version of the primary site.

    - **I'm installing a stand-alone primary site:**

      On the **Primary Site Installation** page, select **Install the primary site as a stand-alone site**, and then choose **Next**.

    - **I'm installing a child primary site:**

      On the **Primary Site Installation** page, select **Join the primary site to an existing hierarchy**. Then specify the FQDN for the central administration site, and choose **Next**.

12. On the **Database Information** page, specify the following information:

    - **SQL Server name (FQDN)**: By default, this value is set to the site server computer.

      If you use a custom port, add that port to the FQDN of the SQL Server. Follow the FQDN of the SQL Server with a comma and then the port number. For example, for server *SQLServer1.fabrikam.com*, use the following to specify port *1551*: `SQLServer1.fabrikam.com,1551`

    - **Instance name**: By default, this value is blank. It uses the default instance of SQL on the site server computer.

- **Database name**: By default, this value is set to `CM_<Sitecode>`. You can customize this value.
- **Service Broker Port**: By default, this value is set to use the default SQL Server Service Broker (SSB) port of 4022. SQL uses it to communicate directly to the site database at other sites.

13. On the second **Database Information** page, you can specify custom locations for the SQL Server data file and the SQL Server log file for the site database:
    - By default, it uses the default file locations for SQL Server.
    - When you use a SQL Server cluster, the option to specify custom file locations isn't available.
    - The prerequisite checker doesn't run a check for free disk space for custom file locations.
14. On the **SMS Provider Settings** page, specify the FQDN for the server where you want to install the SMS Provider.
    - By default, it specifies the site server.
    - After the site installs, you can configure additional SMS Providers. For more information, see Plan for the SMS Provider.
15. On the **Client Communication Settings** page, choose whether to configure all site systems to accept only HTTPS communication from clients or for the communication method to be configured for each site system role.

    When you select **All site system roles accept only HTTPS communication from clients**, the client computer must have a valid PKI certificate for client authentication. For more information, see PKI certificate requirements.

    > **NOTE**
    > This step only applies when you install a primary site. If you're installing a central administration site, skip this step.

16. On the **Site System Roles** page, choose whether to install a management point or distribution point. For each role that you choose to have installed by Setup:
    - Enter the **FQDN** for the server that will host the role. Then choose the client connection method that the server will support: HTTP or HTTPS.
    - If you selected **All site system roles accept only HTTPS communication from clients** on the previous page, the client connection settings are automatically configured for HTTPS. You can't change this setting unless you go back to the previous page.

    > **NOTE**
    > This step only applies when you install a primary site. If you're installing a central administration site, skip this step.

    > **NOTE**
    > To install site system roles, Setup uses the **site system installation account**. By default, this uses the primary site's computer account. This account must be a local administrator on a remote computer to install the site system role. If this account lacks the required permissions, uncheck the site system roles and install them later from within the Configuration Manager console, after configuring additional accounts to use as site system installation accounts. For more information, see Accounts.

17. On the **Usage Data** page, review the information about data that Microsoft collects, and then choose **Next**.

For more information, see Diagnostics and usage data.

18. The **Service Connection Point Setup** page is only available during the following scenarios:

    - When you're installing a stand-alone primary site.
    - When you're installing a central administration site.

    > **NOTE**
    > If you're installing a child primary site, skip this step.

    If you're installing a central administration site as part of a site expansion scenario, and this role is already installed at the stand-alone primary site, first uninstall this role from the stand-alone primary site. Only one instance of this role is permitted in a hierarchy, and it's only supported at the top-tier site of the hierarchy.

    After you select a configuration for the **Service Connection Point**, choose **Next**. After Setup completes, you can change this configuration from within the Configuration Manager console. For more information, see About the service connection point.

19. On the **Settings Summary** page, review the setting that you've selected. When you're ready, choose**Next** to start the Prerequisite Checker.

20. On the **Prerequisite Installation Check** page, it lists any problems that the checker can identify.

    - When the Prerequisite Checker finds a problem, choose an item in the list for details about how to resolve the problem.
    - Before you can continue to install the site, resolve **Failed** items. Also try to resolve items with a status of **Warning**, but they don't block the installation of the site.
    - After resolving issues, choose **Run Check** to rerun the Prerequisite Checker.

      When the Prerequisite Checker runs, and no checks receive a **Failed** status, you can choose **Begin Install** to start the site installation.

    > **TIP**
    > In addition to the feedback that the wizard provides, you can find additional information about prerequisite issues in the **ConfigMgrPrereq.log** file. It's in the root of the system drive of the computer on which you're installing the site. For more information, see List of prerequisite checks.

21. On the **Installation** page, Setup displays the installation status. When the core site server installation is complete, you can **Close** the installation wizard. When you close the wizard, the installation and initial site configurations continue in the background.

    - You can connect a Configuration Manager console to the site before Setup is complete. This console connects as read-only, and lets you view objects and settings, but you can't modify anything.
    - After Setup completes, you can connect a console that can edit objects and settings.

Expand a stand-alone primary site

When you've installed a stand-alone primary site as your first site, you have the option later to expand that site into a larger hierarchy by installing a central administration site.

When you expand a stand-alone primary site, you install a new central administration site that uses the existing stand-alone primary site database as a reference. After the new central administration site installs, the stand-alone

primary site functions as a child primary site.

- You can only expand a stand-alone primary site into a new hierarchy.
- You can only expand one stand-alone primary site into a specific hierarchy. You can't use this option to join additional stand-alone primary sites into the same hierarchy. Instead, use the Migration Wizard to migrate data from one hierarchy into another. For more information, see Migrate data between hierarchies.
- After you expand a stand-alone site into a hierarchy with a central administration site, you can add additional child primary child sites.
- To remove a primary site from a hierarchy with a central administration site, first uninstall the primary site.

To expand the site, use the Configuration Manager Setup Wizard to install a new central administration site with the following caveats:

- Install the central administration site by using the same version of Configuration Manager as the stand-alone primary site.
- On the **Getting Started** page of the Setup Wizard, select the option to install a central administration site. At a later stage of Setup, you'll choose an option to expand an existing stand-alone primary site.
- When you configure the **Client Language Selection** page for the new central administration site, select the same client languages that are configured for the stand-alone primary site that you're expanding.
- On the **Site Installation** page, select the option to expand the stand-alone primary site.

To expand a stand-alone primary site, first see the prerequisites to expand a site. Then use the procedure To install a primary or central administration site earlier in this article.

Install a secondary site

Use the Configuration Manager console to install a secondary site.

- If the console you use isn't connected to the primary site that will be the parent site to the new secondary site, the command to install the site is replicated to the correct primary site.
- Before starting the site installation, make sure that your user account has the prerequisite permissions. Also make sure that the server that will host the new secondary site meets all the prerequisites for use as a secondary site server.
- When you install the secondary site, Configuration Manager configures the new site to use the client communication ports that are configured at the parent primary site.

Process to install a secondary site

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. Select the site that will be the parent primary site of the new secondary site.
2. To start the **Create Secondary Site Wizard**, choose **Create Secondary Site** in the ribbon.
3. On the **Before You Begin** page, confirm that the primary site that's listed is the site that you want to be the parent of the new secondary site. Then choose **Next**.
4. On the **General** page, specify the following settings:
   - **Site code**: Each site code in a hierarchy must be unique. Use three alpha-numeric digits: A through Z and 0 through 9. Because the site code is used in folder names, don't use Windows-reserved names, including:
     - AUX

- CON
- NUL
- PRN
- SMS

> **NOTE**
> Setup doesn't verify whether the site code that you specify is already in use, or if it's a reserved name.

- **Site server name**: This value is the FQDN of the server where the new secondary site will install.
- **Site name**: Each site requires this friendly name, which can help you identify the site.
- **Installation folder**: This folder is the path to the Configuration Manager installation. You can't change the location after the site installs. The path can't contain Unicode characters or trailing spaces.

> **IMPORTANT**
> After you specify details on this page, you can choose **Summary** to go directly to the **Summary** page of the wizard. This action uses the default settings for the remainder of the secondary site options.
>
> - Only use this option when you're familiar with the default settings in this wizard, and they're the settings you want to use.
> - When you use the default settings, boundary groups aren't associated with the distribution point. Until you configure boundary groups that include the secondary site server, clients won't use the distribution point that's installed on this secondary site as a content source location.

5. On the **Installation Source Files** page, choose how the secondary site computer obtains source files for installing the site.

   When you use CD.Latest source files that are shared on the network or copied locally to the target secondary site server:

   - **Version 1802 and earlier**
     - The CD.Latest source file location includes a folder named **Redist**. Move this **Redist** folder as a subfolder under the **SMSSETUP** folder.

       > **NOTE**
       > If hash mismatch errors occur during setup, update the **Redist** folder. Use the Setup Downloader to get the latest files. For any files that cause a hash mismatch error, also copy them from the updated **Redist** folder to the **SMSSETUP\BIN\X64** folder.

   - **Version 1806 and later**
     - The CD.Latest source file location includes a folder named **Redist**. Move this **Redist** folder as a subfolder under the **SMSSETUP** folder.
     - Copy the following files from the **Redist** folder to the **SMSSETUP\BIN\X64** folder:
       - SharedManagementObjects.msi
       - SQLSysClrTypes.msi
       - sqlncli.msi
   - If any of the files from **Redist** aren't available, Setup fails to install the secondary site.

- The computer account of the secondary site server must have **Read** permissions to the source file folder and share.

6. On the **SQL Server Settings** page, specify the version of SQL Server to use, and then configure related settings.

> **NOTE**
> Setup doesn't validate the information that you enter on this page until it starts the installation. Before you continue, verify these settings.

- **Install and configure a local copy of SQL Express on the secondary site computer**
  - **SQL Server Service port**: Specify the SQL Server service port for SQL Server Express to use. The service port is typically configured to use TCP port 1433, but you can configure another port.
  - **SQL Server Broker port**: Specify the SQL Server Service Broker (SSB) port for SQL Server Express to use. The Service Broker is typically configured to use TCP port 4022, but you can configure a different port. Specify a valid port that no other site or service is using, and that no firewall restrictions are blocking.
- **Use an existing SQL Server instance**
  - **SQL Server FQDN**: Review the FQDN for the computer running SQL Server. You must use a local server running SQL Server to host the secondary site database, and you can't modify this setting.
  - **SQL Server instance**: Specify the instance of SQL Server to use as the secondary site database. Leave this option blank to use the default instance.
  - **ConfigMgr site database name**: Specify the name to use for the secondary site database.
  - **SQL Server Broker port**: Specify the SQL Server Service Broker (SSB) port for SQL Server to use. Specify a valid port that no other site or service is using, and that no firewall restrictions block.

> **TIP**
> For a list of the SQL Server versions that System Center Configuration Manager supports, see Supported SQL Server versions.

7. On the **Distribution Point** page, configure settings for the distribution point that will be installed on the secondary site server.

- **Required settings:**
  - **Specify how client devices communicate with the distribution point**: Choose between HTTP and HTTPS.
  - **Create a self-signed certificate or import a PKI client certificate**: Choose between using a self-signed certificate or importing a certificate from your PKI. A self-signed certificate lets you also allow anonymous connections from Configuration Manager clients to the content library. The certificate is used to authenticate the distribution point to a management point before the distribution point sends status messages. For more information, see PKI certificate requirements.

- **Optional settings:**
  - **Install and configure IIS if required by Configuration Manager**: Select this setting to let Configuration Manager install and configure Internet Information Services (IIS) on the server, if it's not already installed. IIS is required on all distribution points.

    > **NOTE**
    > Although this setting is optional, IIS must be installed on the server before a distribution point can be installed successfully.

  - **Enable and configure BranchCache for this distribution point**
  - **Description**: This value is a friendly description for the distribution point to help you recognize it.
  - **Enable this distribution point for prestaged content**

8. On the **Drive Settings** page, specify the drive settings for the secondary site distribution point.

   You can configure up to two disk drives for the content library and two disk drives for the package share. However, Configuration Manager can use additional drives when the first two reach the configured drive space reserve. The **Drive Settings** page is where you configure the priority for the disk drives and the amount of free disk space to remain on each disk drive.

   - **Drive space reserve (MB)**: The value that you configure for this setting determines the amount of free space on a drive before Configuration Manager chooses a different drive and continues the copy process to that drive. Content files can span multiple drives.
   - **Content Locations**: Specify the content locations for the content library and package share. Configuration Manager copies content to the primary content location until the amount of free space reaches the value that's specified for **Drive space reserve (MB)**.

   By default, the content locations are set to **Automatic**. The primary content location is set to the disk drive that has the most disk space at installation time. The secondary location is set to the disk drive that has the most free disk space after the primary drive. When the primary and secondary drives reach the drive space reserve, Configuration Manager selects another available drive with the most free disk space and continues the copy process.

9. On the **Content Validation** page, specify whether to validate the integrity of content files on the distribution point.

   - When you enable content validation on a schedule, Configuration Manager starts the process at the scheduled time. All content on the distribution point is verified.
   - You can also configure the **Content validation priority**.
   - To view the results of the content validation process, in the Configuration Manager console, go to the **Monitoring** workspace, expand **Distribution Status**, and select the **Content Status** node. It displays the content for each package type. These types include applications, software update packages, and boot images.

10. On the **Boundary Groups** page, manage the boundary groups that this distribution point is assigned to:

    - During content deployment, clients must be in a boundary group that's associated with the distribution point to use it as a source location for content.
    - You can select the **Allow fallback source location for content** option to allow clients outside

these boundary groups to fall back and use the distribution point as a source location for content when no preferred distribution points are available.

For more information, see the Fundamental concepts for content management.

11. On the **Summary** page, verify the settings, and then choose **Next** to install the secondary site. When the wizard presents the **Completion** page, you can close the wizard. The secondary site installation continues in the background.

How to verify the secondary site installation status

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. Select the secondary site that you're installing, and then choose **Show Install Status** in the ribbon.

> **TIP**
> When you install more than one secondary site at a time, the Prerequisite Checker runs against a single site at a time. It must finish a site before it starts to check the next site.

Use a command-line to install System Center Configuration Manager sites

9/11/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can run System Center Configuration Manager Setup at a command prompt to install a variety of site types.

Supported tasks for command-line installations

This method of running Setup supports the following site installation and site maintenance tasks:

- **Install a central administration site or primary site from a command prompt**
  View Command-line options for Setup
- **Modify the languages in use at a central administration site or primary site**
  To modify the languages that are installed at a site from a command prompt (including languages for mobile devices), you must:
  - Run Setup from **<ConfigMgrInstallationPath>\Bin\X64** on the site server,
  - Use the **/MANAGELANGS** command-line option,
  - Specify a language script file that specifies the languages you want to add or remove,

    For example, use the following command syntax: **setupwpf.exe /MANAGELANGS <language script file>**

    To create the language script file, use the information in Command line options to manage languages
- **Use an installation script file for unattended site installations or site recovery**
  You can run Setup from a command prompt by using an installation script, and you run an unattended site installation. You can also use this option to recover a site.

  To use a script with Setup:
  - Run Setup with the command line-option **/SCRIPT** and specify a script file.
  - The script file must be configured with required keys and values.

    For an unattended installation of a central administration site or primary site, the script file must have the following sections:
  - Identification
  - Options
  - SQLConfigOptions
    - HierarchyOptions
  - CloudConnectorOptions

    To recover a site, you must also include the following sections of the script file:
  - Identification

- Recovery

For more information, see Unattended site recovery for Configuration Manager.

For a list of keys and values to use in an unattended installation script file, see Unattended Setup script file keys.

About the command-line script file

For unattended installations of Configuration Manager, you can run Setup with the command-line option **/SCRIPT**, and specify a script file that contains installation options. The following tasks are supported by using this method:

- Install a central administration site
- Install a primary site
- Install a configuration Manager console
- Recover a site

> **NOTE**
> You cannot use the unattended script file to upgrade an evaluation site to a licensed installation of Configuration Manager.

The CDLatest key name

When you use media from the CD.Latest folder to run a scripted install of the following four installation options, your script must include the **CDLatest** key with a value of **1**:

- Install a new central administration site
- Install a new primary site
- Recover a central administration site
- Recover a primary site

This value is not supported for use with installation media that you get from the Microsoft Volume License site. See command-line options for information on how to use this key name in the script file.

Create the script

The installation script is automatically created when you run Setup to install a site using the user interface. When you confirm the settings on the **Summary** page of the wizard, the following happens:

- Setup creates the script **%TEMP%\ConfigMgrAutoSave.ini**. You can rename this file before you use it, but it must retain the .ini file extension.
- The unattended installation script contains the settings that you selected in the wizard.
- After the script is created, you can modify the script to install other sites in your hierarchy.
- You can then use this script to perform an unattended setup of Configuration Manager.

This script file provides the same information that the Setup Wizard prompts for, except that there are no default settings.
You must specify all values for the Setup keys that apply to the type of installation that you are using.

When Setup creates the unattended installation script, it's populated with the product key value that you enter during Setup. This can be a valid product key, or **EVAL** when you install an evaluation version of Configuration Manager. The product key value in the script is populated so that the prerequisite check can finish.

When Setup starts the actual site installation, the automatically created script is written to again to clear the product key value in the script that it creates. Before using the script for an unattended installation of a new site, you can edit the script to provide a valid product key or to specify an evaluation installation of Configuration Manager.

Section names, key names, and values

The script contains section names, key names, and values. Note the following information:

- Required section key names vary depending on the installation type that you are scripting.
- The order of the keys within sections and the order of sections within the file is not important.
- The keys are not case-sensitive.
- When you provide values for keys, the name of the key must be followed by an equal sign (=) and the value for the key.

> **TIP**
> To view the full set of options, see Command-line options for Setup and scripts.

Use the /SCRIPT Setup command-line option

- You must use a Setup script file and specify the file name after the **/SCRIPT** Setup command-line option. Note the following information:
  - The name of the file must have the **.ini** file name extension.
  - When you reference the Setup script file at the command prompt, you must provide the full path to the file. For example, if your Setup initialization file is named Setup.ini, and it is stored in the C:\Setup folder, at the command prompt, type: **setup /script c:\setup\setup.ini**.
- The account that runs Setup must have **Administrator** rights on the computer. When you run Setup with the unattended script, open the Command Prompt window by using the **Run as administrator** option.

Command-line options for Configuration Manager setup

8/22/2019 • 28 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the following information to configure scripts or to install Configuration Manager from a command line.

Command-line options for setup

Run setup from the `\BIN\X64` directory of the Configuration Manager installation path on the site server.

`/DEINSTALL`

Uninstall the site. Run setup from the site server computer.

`/DONTSTARTSITECOMP`

Install a site, but prevents the Site Component Manager service from starting. Until the Site Component Manager service starts, the site isn't active. The Site Component Manager is responsible for installing and starting the SMS_Executive service, and for additional processes at the site. After the site install is finished, when you start the Site Component Manager service, it installs the SMS_Executive service and additional processes that are necessary for the site to operate.

`/HIDDEN`

Hide the user interface during setup. Use this option only in conjunction with the **/SCRIPT** option. The unattended script file must provide all required options or setup fails.

`/NOUSERINPUT`

Disable user input during setup, but displays the setup wizard. Use this option only in conjunction with the **/SCRIPT** option. The unattended script file must provide all required options or setup fails.

`/RESETSITE`

Run a site reset that resets the database and service accounts for the site.

For more information, see Run a site reset.

`/TESTDBUPGRADE`

Run a test on a backup of the site database to make sure that the database can upgrade.

> **IMPORTANT**
> Don't run this command-line option on your production site database. Running this command-line option on your production site database upgrades the site database and could render your site inoperable.

Usage

Provide the instance name and database name for the site database. If you specify only the database name, setup uses the default instance name.

`/TESTDBUPGRADE <Instance name>\<Database name>`

`/TESTDBUPGRADE CM_ABC`

`/TESTDBUPGRADE Named\CM_ABC`

`/UPGRADE`

Run an unattended upgrade of a site. Specify the product key including the dashes (`-`). Also specify the path to the previously downloaded setup prerequisite files.

For more information about setup prerequisite files, see Setup Downloader.

Usage

```
setupwpf.exe /UPGRADE xxxxx-xxxxx-xxxxx-xxxxx-xxxxx <path to external component files>
```

`/SCRIPT`

Run an unattended installation. Use a setup initialization file with this option. For more information about how to run setup unattended, see Install sites using a command line.

Usage

```
/SCRIPT <setup script path>
```

`/SDKINST`

Install the SMS Provider on the specified computer. Provide the fully qualified domain name (FQDN) for the SMS Provider computer. For more information about the SMS Provider, see Plan for the SMS Provider.

Usage

```
/SDKINST <SMS Provider FQDN>
```

`/SDKDEINST`

Uninstall the SMS Provider on the specified computer. Provide the FQDN for the SMS Provider computer.

Usage

```
/SDKDEINST <SMS Provider FQDN>
```

`/MANAGELANGS`

Manage the languages that are installed at a previously installed site. Provide the location for the language script file that contains the language settings. For more information, see the Command-line options to manage languages section.

Usage

```
/MANAGELANGS <Language script path>
```

Command-line options to manage languages

Identification

- **Key name:** Action
  - **Required:** Yes
  - **Values:** `ManageLanguages`
  - **Details:** Manages the server, client, and mobile client language support at a site.

Options

- **Key name:** AddServerLanguages
  - **Required:** No
  - **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH

- **Details:** Specifies the server languages that will be available for the Configuration Manager console, reports, and Configuration Manager objects. English is available by default.

- **Key name:** AddClientLanguages
  - **Required:** No
  - **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH
  - **Details:** Specifies the languages that will be available to client computers. English is available by default.
- **Key name:** DeleteServerLanguages
  - **Required:** No
  - **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH
  - **Details:** Specifies the languages to remove, and which will no longer be available for the Configuration Manager console, reports, and Configuration Manager objects. English is available by default, you can't remove it.
- **Key name:** DeleteClientLanguages
  - **Required:** No
  - **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH
  - **Details:** Specifies the languages to remove, and which will no longer be available to client computers. English is available by default, you can't remove it.
- **Key name:** MobileDeviceLanguage
  - **Required:** Yes
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether the mobile device client languages are installed.
- **Key name:** PrerequisiteComp
  - **Required:** Yes
  - **Values:**
    - `0` = Download
    - `1` = Already downloaded
  - **Details:** Specifies whether setup prerequisite files have already been downloaded. For example, if you use a value of `0`, setup downloads the files.
- **Key name:** PrerequisitePath
  - **Required:** Yes
  - **Values:** <*Path to setup prerequisite files*>

- **Details:** Specifies the path to the setup prerequisite files. Depending on the **PrerequisiteComp** value, setup uses this path to store downloaded files or to locate previously downloaded files.

Unattended setup script file keys

Use the following sections to help you create your script for unattended setup. The lists show:

- The available setup script keys and their corresponding values
- If they're required
- Which type of installation they're used for
- A short description of the key

Unattended install for a central administration site (CAS)

Use the following details to install a CAS by using an unattended setup script file.

Identification

- **Key name:** Action
  - **Required:** Yes
  - **Values:** `InstallCAS`
  - **Details:** Installs a CAS.
- **Key name:** CDLatest
  - **Required:** Yes, only when using media from the CD.Latest folder.
  - **Values:**
    - `1` = you're using media from CD.Latest
    - Any value other than 1 = you're not using CD.Latest media
  - **Details:** When you install or recover a primary site or CAS, and you run setup from the CD.Latest folder, include this key and value. This value informs setup that you're using media from CD.Latest.

Options

- **Key name:** ProductID
  - **Required:** Yes
  - **Values:**
    - `<xxxxx-xxxxx-xxxxx-xxxxx-xxxxx>` = a valid product key with dashes
    - `Eval` = install the evaluation version of Configuration Manager
  - **Details:** Specifies the Configuration Manager installation product key, including the dashes.
- **Key name:** SiteCode
  - **Required:** Yes
  - **Values:** <*Site code*>, for example, `ABC`
  - **Details:** Specifies three alphanumeric characters that uniquely identify the site in your hierarchy.
- **Key name:** Site name
  - **Required:** Yes
  - **Values:** <*Site name*>

- **Details:** Specifies the name for this site.

- **Key name:** SMSInstallDir
  - **Required:** Yes
  - **Values:** <*Configuration Manager installation path*>
  - **Details:** Specifies the installation folder for the Configuration Manager program files.
- **Key name:** SDKServer
  - **Required:** Yes
  - **Values:** <*SMS Provider FQDN*>
  - **Details:** Specifies the FQDN for the server that will host the SMS Provider. You can configure additional SMS Providers for the site after the initial installation.
- **Key name:** PrerequisiteComp
  - **Required:** Yes
  - **Values:**
    - `0` = Download
    - `1` = Already downloaded
  - **Details:** Specifies whether setup prerequisite files have already been downloaded. For example, if you use a value of `0`, setup downloads the files.
- **Key name:** PrerequisitePath
  - **Required:** Yes
  - **Values:** <*Path to setup prerequisite files*>
  - **Details:** Specifies the path to the setup prerequisite files. Depending on the **PrerequisiteComp** value, setup uses this path to store downloaded files or to locate previously downloaded files.
- **Key name:** AdminConsole
  - **Required:** Yes
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether to install the Configuration Manager console.
- **Key name:** JoinCEIP

  > **NOTE**
  > Starting in Configuration Manager version 1802 the CEIP feature is removed from the product.

  - **Required:** Yes
  - **Values:**

    - `0` = Don't join
    - `1` = Join
  - **Details:** Specifies whether to join the Customer Experience Improvement Program (CEIP).
- **Key name:** AddServerLanguages
  - **Required:** No
  - **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH
  - **Details:** Specifies the server languages that will be available for the Configuration Manager console, reports, and Configuration Manager objects. English is available by default.
- **Key name:** AddClientLanguages
  - **Required:** No
  - **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH
  - **Details:** Specifies the languages that will be available to client computers. English is available by default.
- **Key name:** DeleteServerLanguages
  - **Required:** No
  - **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH
  - **Details:** Modifies a site after it's installed. Specifies the languages to remove, and which will no longer be available for the Configuration Manager console, reports, and Configuration Manager objects. English is available by default, you can't remove it.
- **Key name:** DeleteClientLanguages
  - **Required:** No
  - **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH
  - **Details:** Modifies a site after it's installed. Specifies the languages to remove, and which will no longer be available to client computers. English is available by default, you can't remove it.
- **Key name:** MobileDeviceLanguage
  - **Required:** Yes
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether the mobile device client languages are installed.

SQLConfigOptions

- **Key name:** SQLServerName
  - **Required:** Yes

- **Values:** <*SQL server name*>
- **Details:** Specifies the name of the server or clustered instance that's running SQL Server to host the site database.

- **Key name:** DatabaseName
  - **Required:** Yes
  - **Values:** <*Site database name*> or <*Instance name*>\<*Site database name*>
  - **Details:** Specifies the name of the SQL Server database to create, or the SQL Server database to use, when setup installs the CAS database.

    > **IMPORTANT**
    > If you don't use the default instance, specify the instance name and site database name.

- **Key name:** SQLSSBPort
  - **Required:** No
  - **Values:** <*SSB port number*>
  - **Details:** Specifies the SQL Server Service Broker (SSB) port that SQL Server uses. By default, SSB uses TCP port 4022, but you can use a different port.
- **Key name:** SQLDataFilePath
  - **Required:** No
  - **Values:** <*Path to database .mdb file*>
  - **Details:** Specifies an alternate location to create the database .mdb file.
- **Key name:** SQLLogFilePath
  - **Required:** No
  - **Values:** <*Path to database .ldf file*>
  - **Details:** Specifies an alternate location to create the database .ldf file.

CloudConnectorOptions

- **Key name:** CloudConnector
  - **Required:** Yes
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether to install a service connection point at this site. Because you can only install the service connection point at the top-tier site of a hierarchy, set this value to `1` for a child primary site.
- **Key name:** CloudConnectorServer
  - **Required:** Required when **CloudConnector** equals 1
  - **Values:** <*Service connection point server FQDN*>

- **Details:** Specifies the FQDN of the server that will host the service connection point site system role.

- **Key name:** UseProxy
  - **Required:** Required when **CloudConnector** equals 1
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether the service connection point uses a proxy server.
- **Key name:** ProxyName
  - **Required:** Required when **UseProxy** equals 1
  - **Values:** <*Proxy server FQDN*>
  - **Details:** Specifies the FQDN of the proxy server that the service connection point uses.
- **Key name:** ProxyPort
  - **Required:** Required when **UseProxy** equals 1
  - **Values:** <*Port number*>
  - **Details:** Specifies the port number to use for the proxy port.

SABranchOptions

- **Key name:** SAActive
  - **Required:** No
  - **Values:**
    - `0` = You don't have Software Assurance
    - `1` = Software Assurance is active
  - **Details:** Specify if you have active Software Assurance. For more information, see Product and licensing FAQ.
- **Key name:** CurrentBranch
  - **Required:** No
  - **Values:**
    - `0` = Install the LTSB
    - `1` = Install current branch
  - **Details:** Specify whether to use Configuration Manager current branch or long-term servicing branch (LTSB). For more information, see Which branch of Configuration Manager should I use?.

Unattended install for a primary site

Use the following details to install a primary site by using an unattended setup script file.

Identification

- **Key name:** Action

- **Required:** Yes
- **Values:** `InstallPrimarySite`
- **Details:** Installs a primary site.

- **Key name:** CDLatest
  - **Required:** Yes, only when using media from the CD.Latest folder.
  - **Values:**
    - `1` = you're using media from CD.Latest
    - Any value other than 1 = you're not using CD.Latest media
  - **Details:** When you install or recover a primary site or CAS, and you run setup from the CD.Latest folder, include this key and value. This value informs setup that you're using media from CD.Latest.

Options

- **Key name:** ProductID
  - **Required:** Yes
  - **Values:**
    - `<xxxxx-xxxxx-xxxxx-xxxxx-xxxxx>` = a valid product key with dashes
    - `Eval` = install the evaluation version of Configuration Manager
  - **Details:** Specifies the Configuration Manager installation product key, including the dashes.
- **Key name:** SiteCode
  - **Required:** Yes
  - **Values:** <*Site code*>
  - **Details:** Specifies three alphanumeric characters that uniquely identify the site in your hierarchy.
- **Key name:** SiteName
  - **Required:** Yes
  - **Values:** <*Site name*>
  - **Details:** Specifies the name for this site.
- **Key name:** SMSInstallDir
  - **Required:** Yes
  - **Values:** <*Configuration Manager installation path*>
  - **Details:** Specifies the installation folder for the Configuration Manager program files.
- **Key name:** SDKServer
  - **Required:** Yes
  - **Values:** <*SMS Provider FQDN*>
  - **Details:** Specifies the FQDN for the server that will host the SMS Provider. You can configure additional SMS Providers for the site after the initial installation.

- **Key name:** PrerequisiteComp
  - **Required:** Yes
  - **Values:**
    - `0` = Download
    - `1` = Already downloaded
  - **Details:** Specifies whether setup prerequisite files have already been downloaded. For example, if you use a value of `0`, setup downloads the files.
- **Key name:** PrerequisitePath
  - **Required:** Yes
  - **Values:** <*Path to setup prerequisite files*>
  - **Details:** Specifies the path to the setup prerequisite files. Depending on the **PrerequisiteComp** value, setup uses this path to store downloaded files or to locate previously downloaded files.
- **Key name:** AdminConsole
  - **Required:** Yes
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether to install the Configuration Manager console.
- **Key name:** JoinCEIP

  > **NOTE**
  > Starting in Configuration Manager version 1802 the CEIP feature is removed from the product.

  - **Required:** Yes
  - **Values:**
    - `0` = Don't join
    - `1` = Join
  - **Details:** Specifies whether to join the CEIP.
- **Key name:** ManagementPoint
  - **Required:** No
  - **Values:** <*Management point site server FQDN*>
  - **Details:** Specifies the FQDN of the server that will host the management point site system role.
- **Key name:** ManagementPointProtocol
  - **Required:** No
  - **Values:** `HTTPS` or `HTTP`

- **Details:** Specifies the protocol to use for the management point.

- **Key name:** DistributionPoint
  - **Required:** No
  - **Values:** <*Distribution point site server FQDN*>
  - **Details:** Specifies the FQDN of the server that will host the distribution point site system role.
- **Key name:** DistributionPointProtocol
  - **Required:** No
  - **Values:** `HTTPS` or `HTTP`
  - **Details:** Specifies the protocol to use for the distribution point.
- **Key name:** RoleCommunicationProtocol
  - **Required:** Yes
  - **Values:** `EnforceHTTPS` or `HTTPorHTTPS`
  - **Details:** Specifies whether to configure all site systems to accept only HTTPS communication from clients, or to configure the communication method for each site system role. When you select `EnforceHTTPS`, clients must have a valid public key infrastructure (PKI) certificate for client authentication.
- **Key name:** ClientsUsePKICertificate
  - **Required:** Yes
  - **Values:**
    - `0` = Don't use
    - `1` = Use
  - **Details:** Specifies whether clients will use a client PKI certificate to communicate with site system roles.
- **Key name:** AddServerLanguages
  - **Required:** No
  - **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH
  - **Details:** Specifies the server languages that will be available for the Configuration Manager console, reports, and Configuration Manager objects. English is available by default.
- **Key name:** AddClientLanguages
  - **Required:** No
  - **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH
  - **Details:** Specifies the languages that will be available to client computers. English is available by default.
- **Key name:** DeleteServerLanguages

- **Required:** No
- **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH
- **Details:** Modifies a site after it's installed. Specifies the languages to remove, and which will no longer be available for the Configuration Manager console, reports, and Configuration Manager objects. English is available by default, you can't remove it.

- **Key name:** DeleteClientLanguages
  - **Required:** No
  - **Values:** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK, or ZHH
  - **Details:** Modifies a site after it's installed. Specifies the languages to remove, and which will no longer be available to client computers. English is available by default, you can't remove it.
- **Key name:** MobileDeviceLanguage
  - **Required:** Yes
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether the mobile device client languages are installed.

SQLConfigOptions

- **Key name:** SQLServerName
  - **Required:** Yes
  - **Values:** *<SQL server name>*
  - **Details:** Specifies the name of the server or clustered instance that runs SQL Server to host the site database.
- **Key name:** DatabaseName
  - **Required:** Yes
  - **Values:** *<Site database name>* or *<Instance name>**<Site database name>*
  - **Details:** Specifies the name of the SQL Server database to create or the SQL Server database to use when installing the primary site database.

    > **IMPORTANT**
    > If you don't use the default instance, specify the instance name and site database name.

- **Key name:** SQLSSBPort
  - **Required:** No
  - **Values:** *<SSB port number>*
  - **Details:** Specifies the SSB port that SQL Server uses. By default, SSB uses TCP port 4022, but you can use a different port.

- **Key name:** SQLDataFilePath
  - **Required:** No
  - **Values:** <*Path to database .mdb file*>
  - **Details:** Specifies an alternate location to create the database .mdb file.
- **Key name:** SQLLogFilePath
  - **Required:** No
  - **Values:** <*Path to database .ldf file*>
  - **Details:** Specifies an alternate location to create the database .ldf file.

HierarchyExpansionOption

- **Key name:** CCARSiteServer
  - **Required:** No
  - **Values:** <*Central administration site FQDN*>
  - **Details:** Specifies the CAS that a primary site attaches to when it joins the Configuration Manager hierarchy. Specify the CAS during setup.
- **Key name:** CASRetryInterval
  - **Required:** No
  - **Values:** <*Interval in minutes*>
  - **Details:** Specifies the retry interval in minutes to attempt a connection to the CAS after the connection fails. For example, if the connection to the CAS fails, the primary site waits the number of minutes that you specify for the **CASRetryInterval** value, and then reattempts the connection.
- **Key name:** WaitForCASTimeout
  - **Required:** No
  - **Values:** <*Timeout in minutes from 0 to 100*>
  - **Details:** Specifies the maximum timeout value in minutes for a primary site to connect to the CAS. For example, if a primary site fails to connect to a CAS, the primary site retries the connection to the CAS based on the **CASRetryInterval** value until the **WaitForCASTimeout** period is reached. You can specify a value from `0` to `100`.

CloudConnectorOptions

- **Key name:** CloudConnector
  - **Required:** Yes
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether to install a service connection point at this site. Because you can only install the service connection point at the top-tier site of a hierarchy, set this value to `0` for a child primary site.
- **Key name:** CloudConnectorServer

- **Required:** Required when **CloudConnector** equals 1
- **Values:** <*Service connection point server FQDN*>
- **Details:** Specifies the FQDN of the server that will host the service connection point site system role.

- **Key name:** UseProxy
  - **Required:** Required when **CloudConnector** equals 1
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether the service connection point uses a proxy server.
- **Key name:** ProxyName
  - **Required:** Required when **UseProxy** equals 1
  - **Values:** <*Proxy server FQDN*>
  - **Details:** Specifies the FQDN of the proxy server that the service connection point uses.
- **Key name:** ProxyPort
  - **Required:** Required when **UseProxy** equals 1
  - **Values:** <*Port number*>
  - **Details:** Specifies the port number to use for the proxy port.

SABranchOptions

- **Key name:** SAActive
  - **Required:** No
  - **Values:**
    - `0` = You don't have Software Assurance
    - `1` = Software Assurance is active
  - **Details:** Specify if you have active Software Assurance. For more information, see Product and licensing FAQ.
- **Key name:** CurrentBranch
  - **Required:** No
  - **Values:**
    - `0` = Install the LTSB
    - `1` = Install current branch
  - **Details:** Specify whether to use Configuration Manager current branch or long-term servicing branch (LTSB). For more information, see Which branch of Configuration Manager should I use?.

Unattended recovery for a CAS

Use the following details to recover a CAS by using an unattended setup script file.

Identification

- **Key name:** Action
  - **Required:** Yes
  - **Values:** `RecoverCCAR`
  - **Details:** Recovers a CAS.
- **Key name:** CDLatest
  - **Required:** Yes, only when using media from the CD.Latest folder.
  - **Values:**
    - `1` = you're using media from CD.Latest
    - Any value other than 1 = you're not using CD.Latest media
  - **Details:** When you install or recover a primary site or CAS, and you run setup from the CD.Latest folder, include this key and value. This value informs setup that you're using media from CD.Latest.

RecoveryOptions

- **Key name:** ServerRecoveryOptions
  - **Required:** Yes
  - **Values:**
    - `1` = Recover site server and SQL Server
    - `2` = Recover site server only
    - `4` = Recover SQL Server only
  - **Details:** Specifies whether setup recovers the site server, SQL Server, or both. The following options are also required based on the specified value:
    - **1** or **2**: To recover the site by using a site backup, specify a value for **SiteServerBackupLocation**. If you don't specify a value, setup reinstalls the site without restoring it from a backup set.
    - **4**: The **BackupLocation** key is required when you configure a value of **10** for the **DatabaseRecoveryOptions** key, which is to restore the site database from backup.
- **Key name:** DatabaseRecoveryOptions
  - **Required:** This key is required when the **ServerRecoveryOptions** setting has a value of **1** or **4**.
  - **Values:**
    - `10` = Restore the site database from backup.
    - `20` = Use a site database that you manually recovered with another method.
    - `40` = Create a new database for the site. Use this option when there's no site database backup available. The site recovers global and site data through replication from other sites.
    - `80` = Skip database recovery.
  - **Details:** Specifies how setup recovers the site database in SQL Server.
- **Key name:** ReferenceSite

- **Required:** This key is required when the **DatabaseRecoveryOptions** setting has a value of **40**.
- **Values:** <*Reference site FQDN*>
- **Details:** If the database backup is older than the change-tracking retention period, or when you recover the site without a backup, specify the reference primary site that the CAS uses to recover global data.

  When you don't specify a reference site, and the backup is older than the change-tracking retention period, all primary sites are reinitialized with the restored data from the CAS.

  When you don't specify a reference site, and the backup is within the change-tracking retention period, only changes that are made after the backup are replicated from primary sites. When there are conflicting changes from different primary sites, the CAS uses the first one that it receives.

- **Key name:** SiteServerBackupLocation
  - **Required:** No
  - **Values:** <*Path to site server backup set*>
  - **Details:** Specifies the path to the site server backup set. This key is optional when the **ServerRecoveryOptions** setting has a value of **1** or **2**. Specify a value for the **SiteServerBackupLocation** key to recover the site by using a site backup. If you don't specify a value, setup reinstalls the site without restoring it from a backup set.
- **Key name:** BackupLocation
  - **Required:** This key is required when you configure a value of **1** or **4** for the **ServerRecoveryOptions** key, and you configure a value of **10** for the **DatabaseRecoveryOptions** key.
  - **Values:** <*Path to site database backup set*>
  - **Details:** Specifies the path to the site database backup set.

Options

- **Key name:** ProductID
  - **Required:** Yes
  - **Values:**
    - `<xxxxx-xxxxx-xxxxx-xxxxx-xxxxx>` = a valid product key with dashes
    - `Eval` = install the evaluation version of Configuration Manager
  - **Details:** Specifies the Configuration Manager installation product key, including the dashes.
- **Key name:** SiteCode
  - **Required:** Yes
  - **Values:** <*Site code*>
  - **Details:** Specifies three alphanumeric characters that uniquely identify the site in your hierarchy. Specify the site code that the site used before the failure.
- **Key name:** SiteName
  - **Required:** No
  - **Values:** <*Site name*>

- **Details:** Specifies the name for this site.

- **Key name:** SMSInstallDir
  - **Required:** Yes
  - **Values:** <*Configuration Manager installation path*>
  - **Details:** Specifies the installation folder for the Configuration Manager program files.

- **Key name:** SDKServer
  - **Required:** Yes
  - **Values:** <*SMS Provider FQDN*>
  - **Details:** Specifies the FQDN for the server that hosts the SMS Provider. Specify the server that hosted the SMS Provider before the failure.

    After the initial installation, you can configure additional SMS Providers for the site. For more information about the SMS Provider, see Plan for the SMS Provider.

- **Key name:** PrerequisiteComp
  - **Required:** Yes
  - **Values:**
    - `0` = Download
    - `1` = Already downloaded
  - **Details:** Specifies whether setup prerequisite files have already been downloaded. For example, if you use a value of **0**, setup downloads the files.

- **Key name:** PrerequisitePath
  - **Required:** Yes
  - **Values:** <*Path to setup prerequisite files*>
  - **Details:** Specifies the path to the setup prerequisite files. Depending on the **PrerequisiteComp** value, setup uses this path to store downloaded files or to locate previously downloaded files.

- **Key name:** AdminConsole
  - **Required:** This key is required except when the **ServerRecoveryOptions** setting has a value of **4**.
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether to install the Configuration Manager console.

- **Key name:** JoinCEIP

  > **NOTE**
  > Starting in Configuration Manager version 1802 the CEIP feature is removed from the product.

  - **Required:** Yes

- **Values:**
  - `0` = Don't join
  - `1` = Join
- **Details:** Specifies whether to join the CEIP.

SQLConfigOptions

- **Key name:** SQLServerName
  - **Required:** Yes
  - **Values:** <*SQL server name*>
  - **Details:** Specifies the name of the server or clustered instance that is running SQL Server, and which hosts the site database. Specify the same server that hosted the site database before the failure.
- **Key name:** DatabaseName
  - **Required:** Yes
  - **Values:** <*Site database name*> or <*Instance name*>\<*Site database name*>
  - **Details:** Specifies the name of the SQL Server database to create or the SQL Server database to use when installing the CAS database. Specify the same database name that was used before the failure.

    > **IMPORTANT**
    > If you don't use the default instance, specify the instance name and site database name.
- **Key name:** SQLSSBPort
  - **Required:** Yes
  - **Values:** <*SSB port number*>
  - **Details:** Specifies the SSB port that SQL Server uses. By default, SSB uses TCP port 4022. Specify the same SSB port that was used before the failure.
- **Key name:** SQLDataFilePath
  - **Required:** No
  - **Values:** <*Path to database .mdb file*>
  - **Details:** Specifies an alternate location to create the database .mdb file.
- **Key name:** SQLLogFilePath
  - **Required:** No
  - **Values:** <*Path to database .ldf file*>
  - **Details:** Specifies an alternate location to create the database .ldf file.

CloudConnectorOptions

- **Key name:** CloudConnector
  - **Required:** Yes
  - **Values:**

    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether to install a service connection point at this site. Because you can only install the service connection point at the top-tier site of a hierarchy, this value must be **0** for a child primary site.
- **Key name:** CloudConnectorServer
  - **Required:** Required when **CloudConnector** equals 1
  - **Values:** <*Service connection point server FQDN*>
  - **Details:** Specifies the FQDN of the server that will host the service connection point site system role.
- **Key name:** UseProxy
  - **Required:** Required when **CloudConnector** equals 1
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether the service connection point uses a proxy server.
- **Key name:** ProxyName
  - **Required:** Required when **CloudConnector** equals 1
  - **Values:** <*Proxy server FQDN*>
  - **Details:** Specifies the FQDN of the proxy server that the service connection point uses.
- **Key name:** ProxyPort
  - **Required:** Required when **CloudConnector** equals 1
  - **Values:** <*Port number*>
  - **Details:** Specifies the port number to use for the proxy port.

Unattended recovery for a primary site

Use the following details to recover a primary site by using an unattended setup script file.

Identification

- **Key name:** Action
  - **Required:** Yes
  - **Values:** `RecoverPrimarySite`
  - **Details:** Recovers a primary site.
- **Key name:** CDLatest
  - **Required:** Yes, only when using media from the CD.Latest folder.
  - **Values:**
    - `1` = you're using media from CD.Latest

- Any value other than 1 = you're not using CD.Latest media

- **Details:** When you install or recover a primary site or CAS, and you run setup from the CD.Latest folder, include this key and value. This value informs setup that you're using media from CD.Latest.

RecoveryOptions

- **Key name:** ServerRecoveryOptions
  - **Required:** Yes
  - **Values:**
    - `1` = Recover site server and SQL Server
    - `2` = Recover site server only
    - `4` = Recover SQL Server only
  - **Details:** Specifies whether setup recovers the site server, SQL Server, or both. The following options are also required based on the specified value:
    - **1** or **2**: To recover the site by using a site backup, specify a value for **SiteServerBackupLocation**. If you don't specify a value, setup reinstalls the site without restoring it from a backup set.
    - **4**: The **BackupLocation** key is required when you configure a value of **10** for the **DatabaseRecoveryOptions** key, which is to restore the site database from backup.
- **Key name:** DatabaseRecoveryOptions
  - **Required:** This key is required when the **ServerRecoveryOptions** setting has a value of **1** or **4**.
  - **Values:**
    - `10` = Restore the site database from backup.
    - `20` = Use a site database that you manually recovered with another method.
    - `40` = Create a new database for the site. Use this option when there's no site database backup available. The site recovers global and site data through replication from other sites.
    - `80` = Skip database recovery.
  - **Details:** Specifies how setup recovers the site database in SQL Server.
- **Key name:** SiteServerBackupLocation
  - **Required:** No
  - **Values:** <*Path to site server backup set*>
  - **Details:** Specifies the path to the site server backup set. This key is optional when the **ServerRecoveryOptions** setting has a value of **1** or **2**. Specify a value for the **SiteServerBackupLocation** key to recover the site by using a site backup. If you don't specify a value, setup reinstalls the site without restoring it from a backup set.
- **Key name:** BackupLocation
  - **Required:** This key is required when you configure a value of **1** or **4** for the **ServerRecoveryOptions** key, and configure a value of **10** for the **DatabaseRecoveryOptions** key.
  - **Values:** <*Path to site database backup set*>

- **Details:** Specifies the path to the site database backup set.

Options

- **Key name:** ProductID
  - **Required:** Yes
  - **Values:**
    - `<xxxxx-xxxxx-xxxxx-xxxxx-xxxxx>` = a valid product key with dashes
    - `Eval` = install the evaluation version of Configuration Manager
  - **Details:** Specifies the Configuration Manager installation product key, including the dashes.
- **Key name:** SiteCode
  - **Required:** Yes
  - **Values:** <*Site code*>
  - **Details:** Specifies three alphanumeric characters that uniquely identify the site in your hierarchy. Specify the site code that the site used before the failure.
- **Key name:** SiteName
  - **Required:** No
  - **Values:** <*Site name*>
  - **Details:** Specifies the name for this site.
- **Key name:** SMSInstallDir
  - **Required:** Yes
  - **Values:** <*Configuration Manager installation path*>
  - **Details:** Specifies the installation folder for the Configuration Manager program files.
- **Key name:** SDKServer
  - **Required:** Yes
  - **Values:** <*SMS Provider FQDN*>
  - **Details:** Specifies the FQDN for the server that hosts the SMS Provider. Specify the server that hosted the SMS Provider before the failure. After the initial installation, you can configure additional SMS Providers for the site. For more information about the SMS Provider, see Plan for the SMS Provider.
- **Key name:** PrerequisiteComp
  - **Required:** Yes
  - **Values:**
    - `0` = Download
    - `1` = Already downloaded
  - **Details:** Specifies whether setup prerequisite files have already been downloaded. For example, if you use a value of **0**, setup downloads the files.
- **Key name:** PrerequisitePath

- **Required:** Yes
- **Values:** <*Path to setup prerequisite files*>
- **Details:** Specifies the path to the setup prerequisite files. Depending on the **PrerequisiteComp** value, setup uses this path to store downloaded files or to locate previously downloaded files.

- **Key name:** AdminConsole
  - **Required:** This key is required except when the **ServerRecoveryOptions** setting has a value of **4**.
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether to install the Configuration Manager console.
- **Key name:** JoinCEIP

  > **NOTE**
  > Starting in Configuration Manager version 1802 the CEIP feature is removed from the product.

  - **Required:** Yes
  - **Values:**
    - `0` = Don't join
    - `1` = Join
  - **Details:** Specifies whether to join the CEIP.

SQLConfigOptions

- **Key name:** SQLServerName
  - **Required:** Yes
  - **Values:** <*SQL server name*>
  - **Details:** Specifies the name of the server or clustered instance that runs SQL Server to host the site database. Specify the same server that hosted the site database before the failure.
- **Key name:** DatabaseName
  - **Required:** Yes
  - **Values:** <*Site database name*> or <*Instance name*>\<*Site database name*>
  - **Details:** Specifies the name of the SQL Server database to create or the SQL Server database to use when installing the CAS database. Specify the same database name that was used before the failure.

    > **IMPORTANT**
    > If you don't use the default instance, specify the instance name and site database name.

- **Key name:** SQLSSBPort
  - **Required:** Yes

- **Values:** <*SSB port number*>
- **Details:** Specifies the SSB port that SQL Server uses. By default, SSB uses TCP port 4022. Specify the same SSB port that was used before the failure.

- **Key name:** SQLDataFilePath
  - **Required:** No
  - **Values:** <*Path to database .mdb file*>
  - **Details:** Specifies an alternate location to create the database .mdb file.
- **Key name:** SQLLogFilePath
  - **Required:** No
  - **Values:** <*Path to database .ldf file*>
  - **Details:** Specifies an alternate location to create the database .ldf file.

HierarchyExpansionOptions

- **Key name:** CCARSiteServer
  - **Required:** See details.
  - **Values:** <*Site code for CAS*>
  - **Details:** Specifies the CAS to which a primary site attaches when it joins the Configuration Manager hierarchy. This setting is required if the primary site was attached to a CAS before the failure. Specify the site code that was used for the CAS before the failure.
- **Key name:** CASRetryInterval
  - **Required:** No
  - **Values:** <*Interval in minutes*>
  - **Details:** Specifies the retry interval in minutes to attempt a connection to the CAS after the connection fails. For example, if the connection to the CAS fails, the primary site waits the number of minutes that you specify for the **CASRetryInterval** value, and then attempts the connection again.
- **Key name:** WaitForCASTimeout
  - **Required:** No
  - **Values:** <*Timeout in minutes*>
  - **Details:** Specifies the maximum timeout value in minutes for a primary site to connect to the CAS. For example, if a primary site fails to connect to a CAS, the primary site retries the connection to the CAS based on the **CASRetryInterval** value until the **WaitForCASTimeout** period is reached. You can specify a value of `0` to `100`.

CloudConnectorOptions

- **Key name:** CloudConnector
  - **Required:** Yes
  - **Values:**
    - `0` = Don't install
    - `1` = Install

- **Details:** Specifies whether to install a service connection point at this site. Because you can only install the service connection point at the top-tier site of a hierarchy, this value must be `0` for a child primary site.

- **Key name:** CloudConnectorServer
  - **Required:** Required when **CloudConnector** equals 1
  - **Values:** <*Service connection point server FQDN*>
  - **Details:** Specifies the FQDN of the server that will host the service connection point site system role.
- **Key name:** UseProxy
  - **Required:** Required when **CloudConnector** equals 1
  - **Values:**
    - `0` = Don't install
    - `1` = Install
  - **Details:** Specifies whether the service connection point uses a proxy server.
- **Key name:** ProxyName
  - **Required:** Required when **CloudConnector** equals 1
  - **Values:** <*Proxy server FQDN*>
  - **Details:** Specifies the FQDN of the proxy server that the service connection point uses.
- **Key name:** ProxyPort
  - **Required:** Required when **CloudConnector** equals 1
  - **Values:** <*Port number*>
  - **Details:** Specifies the port number to use for the proxy port.

Install the Configuration Manager console

5/9/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Administrators use the Configuration Manager console to manage the Configuration Manager environment. Each Configuration Manager console can connect to a central administration site (CAS) or to a primary site. You can't connect a Configuration Manager console to a secondary site.

The Configuration Manager console is always installed on the site server for the CAS or a primary site. To install the console separate from site server installation, run the standalone installer.

Prerequisites

- You have local **Administrator** rights on the target computer for the console.
- You have **Read** permissions to the location of the Configuration Manager console installation files.

Source paths

Decide which source path to use:

- ConsoleSetup folder on the site server:
  `<Configuration Manager site server installation path>\Tools\ConsoleSetup`

  When you install a site server, it copies the console installation files and supported language packs for the site to the **Tools\ConsoleSetup** subfolder. Optionally, you can copy the **ConsoleSetup** folder to an alternate location to start the installation. When you update the site, it always keeps its local version up to date.

- Configuration Manager installation media: `<Configuration Manager installation media>\SMSSETUP\BIN\I386`

  Installing the Configuration Manager console from the installation media always installs the English version. This behavior happens even if the site server supports different languages, or the target computer's OS is set to a different language.

When possible, start the console installer from the **ConsoleSetup** folder rather than from the source media.

> **IMPORTANT**
> Don't install the console using the **CD.Latest** source files. It's an unsupported scenario, and may cause problems with the console installation. For more information, see The CD.Latest folder.

If you create a package for installing the console on other computers, make sure the package includes the following files:

- ConsoleSetup.exe
- AdminConsole.msi
- ConfigMgr.AC_Extension.i386.cab (starting in version 1902)
- ConfigMgr.AC_Extension.amd64.cab (starting in version 1902)

Use the Setup Wizard

1. Browse to the source path, and open **ConsoleSetup.exe**.

   > **IMPORTANT**
   > Always install the console by using **ConsoleSetup.exe**. Although you can install the Configuration Manager console by running AdminConsole.msi, this method doesn't run prerequisites or dependency checks. The installation might not install correctly.

2. In the wizard, select **Next**.

3. On the **Site Server** page, enter the fully qualified domain name (FQDN) of the site server to which the Configuration Manager console connects.

4. On the **Installation Folder** page, enter the installation folder for the Configuration Manager console. The folder path can't include trailing spaces or Unicode characters.

5. On the **Customer Experience Improvement Program** page, select whether to join the Customer Experience Improvement Program (CEIP).

   > **NOTE**
   > Starting in Configuration Manager version 1802, the CEIP feature is removed from the product.

6. On the **Ready to Install** page, select **Install**.

Install from a command prompt

> **TIP**
> Installing the Configuration Manager console from a command prompt always installs the English version. This behavior happens even if the target computer's OS is set to a different language. To install the Configuration Manager console in a language other than English, use the Setup Wizard.

ConsoleSetup.exe command-line options

/q

Installs the Configuration Manager console unattended. The **EnableSQM**, **TargetDir**, and **DefaultSiteServerName** options are required when you use this option.

/uninstall

Uninstalls the Configuration Manager console. Specify this option first when you use it with the **/q** option.

LangPackDir

Specifies the path to the folder that contains the language files. You can use **Setup Downloader** to download the language files. If you don't use this option, Setup looks for the language folder in the current folder. If the language folder isn't found, Setup continues to install English only. For more information, see Setup Downloader.

TargetDir

Specifies the installation folder to install the Configuration Manager console. This option is required when you use the **/q** option.

EnableSQM

Specifies whether to join the Customer Experience Improvement Program (CEIP). Use a value of **1** to join the CEIP, and a value of **0** to not join the program. This option is required when you use the **/q** option.

> **IMPORTANT**
>
> Starting in Configuration Manager version 1802, the CEIP feature is removed from the product. Using the parameter will cause the install to fail.

DefaultSiteServerName

Specifies the FQDN of the site server to which the console connects when it opens. This option is required when you use the **/q** option.

Examples

> **IMPORTANT**
>
> For version 1802 and later, don't include the **EnableSQM** parameter

Silent install

```
ConsoleSetup.exe /q TargetDir="%ProgramFiles%\ConfigMgr Console" DefaultSiteServerName=MyServer.Contoso.com
```

Silent install with language packs

```
ConsoleSetup.exe /q TargetDir="C:\Program Files\ConfigMgr Console" DefaultSiteServerName=MyServer.Contoso.com
LangPackDir=C:\Downloads\ConfigMgr
```

Silent uninstall

```
ConsoleSetup.exe /uninstall /q
```

See also

An administrator sees objects in the console based on the permissions assigned to their user account. For more information, see Fundamentals of role-based administration.

For more information on the fundamentals of navigating the Configuration Manager console, see Using the console.

Upgrade an evaluation installation of System Center Configuration Manager to a full installation

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

If you installed System Center Configuration Manager as an evaluation version, after 180 days, the Configuration Manager console becomes read-only until you activate the product from the **Site Maintenance** page in Setup. At any time before or after the 180-day period, you have the option to upgrade an evaluation installation to a full installation.

> **NOTE**
> When you connect a Configuration Manager console to an evaluation installation of Configuration Manager, the console title bar displays the number of days that remain until the evaluation installation expires. The number of days does not automatically refresh and it only updates when you make a new connection to a site.

You can upgrade the following sites that run an evaluation installation:

- Central administration site
- Primary site

Because secondary sites are not treated as evaluation installations, you do not need to modify a secondary site after its primary parent site upgrades to a full installation.

Prerequisites to upgrading an evaluation version to a licensed version:

- You must have a valid product to use during the upgrade.
- Your account must have **Administrator** rights on the computer where the site is installed.

To upgrade an evaluation version of Configuration Manager to a licensed version

1. On the site server, run **Setup.exe** (Configuration Manager setup) from the Configuration Manager installation folder (**%path%\BIN\X64**). You must run the copy of Setup that is located on the site server in the Configuration Manager folder because site maintenance options are not available when you run Setup from installation media.
2. On the **Before You Begin** page, select **Next**.
3. On the **Getting Started** page, select **Perform site maintenance or reset the Site**, and then select **Next**.
4. On the **Site Maintenance** page, select **Upgrade the evaluation edition to a licensed edition**, enter a valid product key, and then select **Next**.
5. On the **Microsoft Software License Terms** page, read and accept the license terms, and then select **Next**.
6. On the **Configuration** page, select **Close** to complete the wizard.

> **NOTE**
> The title bar of a Configuration Manager console that remains connected to the site that you upgrade might indicate that the site is still an evaluation version until you reconnect the console to the site.

Upgrade to Configuration Manager current branch

9/11/2019 • 21 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Do an in-place upgrade to Configuration Manager current branch from a site and hierarchy that runs System Center 2012 Configuration Manager. Before upgrading from System Center 2012 Configuration Manager, you must prepare the sites. This preparation requires you to remove specific configurations that can prevent a successful upgrade. Then follow the upgrade sequence when more than a single site is involved.

> **TIP**
> When managing Configuration Manager site and hierarchy infrastructure, the terms *upgrade*, *update*, and *install* are used to describe three separate concepts. To learn how each term is used, see About upgrade, update, and install.

In-place upgrade paths

The following options are the currently supported in-place upgrade paths:

Upgrade to version 1902

You can upgrade the following to a fully licensed version of System Center Configuration Manager version 1902:

- An evaluation install of System Center Configuration Manager version 1902
- System Center 2012 Configuration Manager with Service Pack 1
- System Center 2012 Configuration Manager with Service Pack 2
- System Center 2012 R2 Configuration Manager
- System Center 2012 R2 Configuration Manager with Service Pack 1

Upgrade to version 1802

You can upgrade the following to a fully licensed version of System Center Configuration Manager version 1802:

- An evaluation install of System Center Configuration Manager version 1802
- System Center 2012 Configuration Manager with Service Pack 1
- System Center 2012 Configuration Manager with Service Pack 2
- System Center 2012 R2 Configuration Manager
- System Center 2012 R2 Configuration Manager with Service Pack 1

For more information, see Frequently asked questions for Configuration Manager branches and licensing.

> **TIP**
> When you upgrade from a System Center 2012 Configuration Manager version to Current Branch, you might be able to streamline your upgrade process. For more information, see the following:
>
> - Baseline and update versions
> - The CD.Latest folder

Unsupported paths

The following paths aren't supported:

- It's not supported to upgrade a technical preview branch to a fully licensed installation. A technical preview version can only upgrade to a later version of the technical preview.
- Migration from a technical preview to a fully licensed version isn't supported.

Upgrade checklists

The following checklists can help you plan a successful upgrade to Configuration Manager.

Before you upgrade

Review these steps before you upgrade to Configuration Manager.

Review your System Center 2012 Configuration Manager environment

Resolve issues as detailed in the following Microsoft Support article: Configuration Manager clients reinstall every five hours because of a recurring retry task and may cause an inadvertent client upgrade.

Make sure your environment meets the supported configurations

- Review the server OS version in use to host site system roles:
  - Some older operating systems supported by System Center 2012 Configuration Manager aren't supported by Configuration Manager current branch. Before the upgrade, remove site system roles on those OS versions. For more information, see Supported operating systems for site system servers.
  - The prerequisite checker for Configuration Manager doesn't verify the prerequisites for site system roles on the site server or on remote site systems
- Review required prerequisites for each computer that hosts a site system role. For example, to deploy an OS, Configuration Manager uses the Windows 10 Assessment and Deployment Kit (Windows ADK). Before you run Setup, you must download and install Windows 10 ADK on the site server and on each computer that runs an instance of the SMS Provider.

For more information about supported platforms and prerequisite configurations, see Supported configurations.

For more information about using the Windows ADK with Configuration Manager, see Infrastructure requirements for OS deployment.

Review the site and hierarchy status and verify that there are no unresolved issues

Before you upgrade a site, resolve all operational issues for the site server, the site database server, and site system roles that are installed on remote computers. A site upgrade can fail because of existing operational problems.

Install all applicable critical updates for operating systems on computers that host the site, the site database server, and remote site system roles

Before you upgrade a site, install any critical updates for each applicable site system. If an update that you install requires a restart, restart the applicable computers before you start the service pack update.

Uninstall the site system roles not supported by Configuration Manager

The following site system roles are no longer used in Configuration Manager. Uninstall them before you upgrade from System Center 2012 Configuration Manager:

- Out of Band Management point
- System Health Validator point

Disable database replicas for management points at primary sites

Configuration Manager can't upgrade a primary site that has a database replica for management points. Disable database replication before you:

- Create a backup of the site database to test the database upgrade

- Upgrade the production site to System Center Configuration Manager

For more information, see the following articles:

- System Center 2012 Configuration Manager: Configure database replicas for management points
- Configuration Manager, current branch: Database replicas for management points

Reconfigure software update points that use NLB

Configuration Manager can't upgrade a site that uses a Network Load Balancing (NLB) cluster to host software update points.

If you use NLB clusters for software update points, use PowerShell to remove the NLB cluster. (Beginning with System Center 2012 Configuration Manager SP1, there was no option in the Configuration Manager console to configure an NLB cluster)

Disable all site maintenance tasks at each site for the duration of that site's upgrade

Before you upgrade to Configuration Manager, disable any site maintenance tasks that might run during the time the upgrade process is active. This list includes but isn't limited to the following tasks:

- Backup Site Server
- Delete Aged Client Operations
- Delete Aged Discovery Data

If a site database maintenance task runs during the upgrade process, the site upgrade can fail.

Before you disable a task, record the schedule of the task so you can restore its configuration after the site upgrade completes.

For more information about site maintenance tasks, see the following articles:

- System Center 2012 Configuration Manager: Planning for site operations
- Configuration Manager, current branch: Reference for maintenance tasks

Run setup prerequisite checker

Before you upgrade a site, run the **Prerequisite Checker** independently from Setup to validate that your site meets the prerequisites. Later, when you upgrade the site, Prerequisite Checker runs again.

If you use the baseline media for version 1606 from the October 2016 release, the independent prerequisite check evaluates the site for upgrade to both the current branch and the long-term servicing branch (LTSB) of Configuration Manager. Because some features aren't supported by the LTSB, you might see entries in the *ConfigMgrPrereq.log* that are like the following examples:

- `INFO: The site is a LTSB edition.`
-
```
Unsupported site system role 'Asset Intelligence synchronization point' for the LTSB edition; Error; Configuration Manager has detected that the 'Asset Intelligence synchronization point' is installed. Asset Intelligence is not supported on the LTSB edition. You must uninstall the Asset Intelligence synchronization point site system role before you can continue.
```

If you plan to upgrade to the current branch, errors for the LTSB edition can be safely ignored. They only apply if you plan to upgrade to the LTSB.

Later, when you run Configuration Manager Setup to do the upgrade, the prerequisite check runs again. It evaluates your site based on the branch of Configuration Manager you choose to install (current branch, or LTSB). If you choose to upgrade to the current branch, it doesn't run the check for features that aren't supported by the LTSB.

For more information, see the Prerequisite checker and List of prerequisite checks.

Download prerequisite files and redistributable files for Configuration Manager

Use **Setup Downloader** to download prerequisite redistributable files, language packs, and the latest product updates for Configuration Manager.

For information, see Setup Downloader.

Plan to manage server and client languages

When you upgrade a site, the site upgrade installs only the language pack versions you select during the upgrade.

- Setup reviews the current language configuration of your site. It then identifies the language packs that are available in the folder where you store previously downloaded prerequisite files.
- You can affirm the selection of the current server and client language packs, or change the selections to add or remove support for languages.
- Only language packs that are available when you run Setup can be selected.

> **NOTE**
> You can't use the language packs from System Center 2012 Configuration Manager to enable languages for a Configuration Manager current branch site.

For more information about language packs, see Language packs.

Review considerations for site upgrades

When you upgrade a site, some features and configurations reset to a default configuration. To help you prepare for these and related changes, see Considerations for upgrading.

Create a backup of the site database at the central administration site and primary sites

Before you upgrade a site, back up the site database to make sure that you have a successful backup to use for disaster recovery.

For more information, see Backup and recovery.

Back up a customized Configuration.mof file

If you use a customized Configuration.mof file to define data classes you use with hardware inventory, create a backup of this file. After the upgrade, restore this file to your site. For more information, see How to extend hardware inventory.

Test the database upgrade process on a copy of the most recent site database backup

Before you upgrade a Configuration Manager central administration site or primary site, test the site database upgrade process on a copy of the site database.

- Test the site database upgrade process. When you upgrade a site, the site database might be modified.
- Although testing the database upgrade isn't required, it can identify problems for the upgrade before your production database is affected
- A failed site database upgrade can render your site database inoperable and might require a site recovery to restore functionality
- Although the site database is shared between sites in a hierarchy, plan to test the database at each applicable site before you upgrade that site
- If you use database replicas for management points at a primary site, disable replication before you create the backup of the site database

Configuration Manager doesn't support the backup of secondary sites, or the test upgrade of a secondary site database.

It's not supported to run a test database upgrade on the production site database. Doing so upgrades the site

database and could render your site inoperable.

For more information, see Test the site database upgrade.

Restart the site server and each computer that hosts a site system role

Do this action to make sure there are no pending actions from a recent installation of updates or from prerequisites.

Upgrade sites

Starting at the top-level site in the hierarchy, run Setup.exe from the Configuration Manager source media.

After the top-level site upgrades, you can begin the upgrade of each child site. Complete the upgrade of each site before you begin to upgrade the next site.

Until all sites in your hierarchy upgrade to Configuration Manager, your hierarchy operates in a mixed version mode.

For information about how to run upgrade, see Upgrade sites.

After you upgrade

Review these steps after you upgrade to Configuration Manager.

Upgrade stand-alone Configuration Manager consoles

By default, when you upgrade a central administration site or primary site, the installation also upgrades the Configuration Manager console that's installed on the site server. Manually upgrade each console that's installed on a computer other than the site server.

> **TIP**
> Close each open console before you start the upgrade.

For more information, see Install Configuration Manager consoles.

Reconfigure database replicas for management points at primary sites

If you use database replicas for management points at primary sites, uninstall the database replicas before you upgrade the site. After you upgrade a primary site, reconfigure the database replica for management points.

For more information, see Database replicas for management points.

Reconfigure any database maintenance tasks you disabled before the upgrade

If you disabled database maintenance tasks at a site before the upgrade, reconfigure those tasks at the site using the same settings that were in place before the upgrade.

Upgrade clients

After all your sites upgrade to Configuration Manager, plan to upgrade clients.

When you upgrade a client, the current client software is uninstalled and the new client software version is installed. To upgrade clients, you can use any method that Configuration Manager supports.

> **TIP**
> When you upgrade the top-level site of a hierarchy, the client installation package on each distribution point in the hierarchy is also updated. When you upgrade a primary site, the client upgrade package that's available from that primary site is updated.

For more information, see How to upgrade clients for Windows computers.

Considerations for upgrading

Automatic actions

When you upgrade to Configuration Manager, the following actions occur automatically:

- A site reset. This action includes a reinstallation of all site system roles.
- If the site is the top-level site of a hierarchy, it updates the client installation package on each distribution point in the hierarchy. The site also updates the default boot images to use the new Windows PE version that's included with the Windows Assessment and Deployment Kit 10. However, the upgrade doesn't upgrade existing media for use with image deployment.
- If the site is a primary site, it updates the client upgrade package for that site.

Manual actions after an upgrade

After you upgrade a site, make sure that you do the following actions:

- Make sure that clients assigned to each primary site upgrade and install the new client version
- Upgrade each Configuration Manager console that connects to the site and that runs on a computer that is remote from the site server
- At primary sites where you use database replicas for management points, reconfigure the database replicas
- After the site upgrades, manually upgrade physical media like ISO files for CDs, DVDs, or USB flash drives. It also includes prestaged media provided to hardware vendors. The site upgrade updates the default boot images, it can't upgrade these media files or devices used external to Configuration Manager.
- Plan to update custom boot images when you don't require the older version of Windows PE.

Actions that affect configurations and settings**

When a site upgrades to Configuration Manager, some configurations and settings don't persist after the upgrade. Some configurations are set to a new default. The following list includes some settings that don't persist or that change:

- **Software Center**
  The following Software Center items are reset to their default values:
  - **Work information** is reset to business hours from **5.00am** to **10.00pm** Monday to Friday.
  - The value for **Computer maintenance** is set to **Suspend Software Center activities when my computer is in presentation mode**.
  - The value for **Remote control** is set to the value in the client settings that are assigned to the computer.
- **Software update summarization schedules**: Custom summarization schedules for software updates or software update groups are reset to the default value of 1 hour. After the upgrade finishes, reset custom summarization values to the required frequency.

Test the site database upgrade

The following information applies only when you're upgrading a prior version like System Center 2012 Configuration Manager to Configuration Manager current branch.

Before you upgrade a site, test a copy of that site's database for the upgrade.

To test the database for an upgrade, you first restore a copy of the site database to an instance of SQL Server that doesn't host a Configuration Manager site. The version of SQL Server that you use to host the database copy must be a version of SQL Server that Configuration Manager supports.

After you restore the site database, on the SQL Server computer, run Configuration Manager Setup from the

source media folder for Configuration Manager. Use the `/TESTDBUPGRADE` command-line option.

For more information, see the following articles:

- Back up a Configuration Manager site
- Command-line options for Setup
- Support for SQL Server versions

> **TIP**
> If you integrate Microsoft Intune with Configuration Manager:
>
> When you run a test database upgrade on copy of the site database that is 5 or more days old, you might receive one of the following messages:
>
> - WARN: Upgrade will force full sync to cloud.
> - ERROR: Database upgrade will force full sync to cloud.
>
> Both can be safely ignored during the testing of a database upgrade. They don't indicate a failure or problem with the test upgrade. Instead, they indicate that during the actual upgrade, data from the **Cloud** database replication group might synchronize with Microsoft Intune.

Test a site database for upgrade

Use the following procedure on each central administration site and primary site that you plan to upgrade:

1. Make a copy of the site database. Then restore that copy to an instance of SQL Server that uses the same edition as your site database, and that doesn't host a Configuration Manager site. For example, if the site database runs on an instance of the Enterprise edition of SQL Server, make sure you restore the database to an instance of SQL Server that also runs the Enterprise edition of SQL Server.

2. After you restore the database copy, run Setup from the source media for Configuration Manager current branch. When you run Setup, use the `/TESTDBUPGRADE` command-line option. If the SQL Server instance that hosts the database copy isn't the default instance, also provide the command-line arguments to identify the instance that hosts the site database copy.

   For example, you plan to upgrade a site database with the database name SMS_ABC. You restore a copy of this site database to a supported instance of SQL Server with the instance name DBTest. To test an upgrade of this copy of the site database, use the following command line: `Setup.exe /TESTDBUPGRADE DBtest\CM_ABC`

   Setup.exe is in the following location on the Configuration Manager source media: `SMSSETUP\BIN\X64`

3. On the instance of SQL Server where you run the database upgrade test, monitor the ConfigMgrSetup.log in the root of the system drive for progress and success:

   - If the test upgrade fails, resolve any issues related to the site database upgrade failure. Then create a new backup of the site database, and test the upgrade of the new copy of the site database.
   - After the process is successful, you can delete the database copy.

     > **NOTE**
     > It's not supported to restore the copy of the site database that you use for the test upgrade for use as a site database at any site.

After you successfully upgrade a copy of the site database, continue with the upgrade of the Configuration Manager site and its site database.

Upgrade sites

You're ready to upgrade your Configuration Manager site after you complete the following tasks:

- Pre-upgrade configurations for your site
- Test the upgrade of the site database on a database copy
- Download prerequisite files and language packs for the version that you plan to install

When you upgrade a site in a hierarchy, you upgrade the top-level site of the hierarchy first. This top-level site is either a central administration site or a stand-alone primary site. After you complete the upgrade of a central administration site, you can upgrade child primary sites in any order that you want. After you upgrade a primary site, you can upgrade that site's child secondary sites, or upgrade additional primary sites before you upgrade any secondary sites.

To upgrade a central administration site or primary site, run Setup from the Configuration Manager source media. Don't run Setup to upgrade secondary sites. Instead, you use the Configuration Manager console to upgrade a secondary site after you complete the upgrade of its primary parent site.

Before you upgrade a site, close the Configuration Manager console on the site server until after the site upgrade is completed. Also, close each Configuration Manager console that runs on computers other than the site server. You can reconnect the console after the site upgrade is completed. However, until you upgrade a Configuration Manager console to the new version of Configuration Manager, that console can't display some objects and information that are available in new version of Configuration Manager.

Upgrade a central administration site or primary site

1. Verify that the user who runs Setup has the following security rights:

   - Local **Administrator** rights on the site server
   - If the site database server is remote from the site server, local **Administrator** rights on it.

2. On the site server, open the following program: `<ConfigMgSourceMedia>\SMSSETUP\BIN\X64\Setup.exe`. This action opens the Configuration Manager Setup wizard.

3. Read the information on the **Before You Begin** page, and then select **Next**.

4. On the **Getting Started** page, select **Upgrade this Configuration Manager site**, and then select **Next**.

5. On the **Product Key** page:

   If you previously installed Configuration Manager Evaluation, you can select **Install the licensed edition of this product**. Then enter your product key for the full installation of Configuration Manager. This action converts the site to the full version.

   You can also specify the **Software Assurance expiration date** of your licensing agreement as a convenient reminder to you of that date. If you don't enter this value during setup, you can specify it later from within the Configuration Manager console.

   > **NOTE**
   > Microsoft doesn't validate the expiration date you entered, and won't use this date for license validation. You can use it as a reminder of your expiration date. Configuration Manager periodically checks for new software updates offered online and your software assurance license status should be current to be eligible to use these additional updates.

   For more information, see Licensing and branches.

6. On the **Microsoft Software License Terms** page, read and accept the license terms, and then select **Next**.

7. On the **Prerequisite Licenses** page, read and accept the license terms for the prerequisite software, and then select **Next**. Setup downloads and automatically installs the software on site systems or clients when it's required. Before you can continue to the next page, agree to all terms.

8. On the **Prerequisite Downloads** page, specify whether Setup downloads the latest content from the internet or use previously downloaded files. This content includes prerequisite redistributable files, language packs, and the latest product updates. If you previously downloaded the files by using Setup Downloader, select **Use previously downloaded files** and specify the download folder. For more information, see Setup Downloader.

   > **NOTE**
   > When you use previously downloaded files, verify that the path to the download folder contains the most recent version of the files.

9. On the **Server Language Selection** page, view the list of languages that are currently installed for the site. Select additional languages that are available at this site for the Configuration Manager console and for reports. You can also clear languages that you no longer want to support at this site. By default, English is selected and can't be removed.

   > **IMPORTANT**
   > Each version of Configuration Manager can't use language packs from a prior version of Configuration Manager. To enable support for a language at a Configuration Manager site that you upgrade, you must use the version of the language pack for that new version. For example, during upgrade from System Center 2012 Configuration Manager to Configuration Manager current branch, if the current branch version of a language pack isn't available with the prerequisite files you download, you can't install support for that language.

10. On the **Client Language Selection** page, view the list of languages that are currently installed for the site. Select additional languages that are available at this site for client computers, or clear languages that you no longer want to support at this site. Specify whether to enable all client languages for mobile device clients, and then click **Next**. By default, English is selected and can't be removed.

11. On the **Settings Summary** page, review the configuration. When you're ready, select**Next** to start Prerequisite Checker to verify server readiness for the upgrade of the site.

12. On the **Prerequisite Installation Check** page, if there are no problems listed, select **Next** to upgrade the site and site system roles.

    If Prerequisite Checker finds a problem, select an item on the list for details about how to resolve the problem. Resolve all items in the list that have an **Error** status before you continue Setup. After you resolve the issue, click **Run Check** to restart prerequisite checking. You can also open the ConfigMgrPrereq.log file in the root of the system drive to review the Prerequisite Checker results. The log file can contain additional information that's not displayed in the user interface. For a list of installation prerequisite rules and descriptions, see Prerequisite Checker.

On the **Upgrade** page, Setup displays the overall progress status. When Setup completes the core site server and site system installation, you can close the wizard. Site configuration continues in the background.

Upgrade a secondary site

1. Verify that the administrative user that runs Setup has the following security rights:

   - Local **Administrator** rights on the secondary site server
   - **Infrastructure Administrator** or **Full Administrator** security role on the parent primary site

- System administrator (**SA**) rights on the site database of the secondary site

2. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and then select the **Sites** node.
3. Select the secondary site that you want to upgrade. On the **Home** tab of the ribbon, in the **Site** group, select **Upgrade**.
4. Select **Yes** to confirm the decision, and to start the upgrade of the secondary site.

The secondary site upgrade runs in the background. After the upgrade is complete, confirm the status in the Configuration Manager console. Select the secondary site server, then on the **Home** tab of the ribbon, in the **Site** group, select **Show Install Status**.

Post-upgrade tasks

After you upgrade a site, you might have to complete additional tasks to finish the upgrade or reconfigure the site. These tasks can include the following items:

- Upgrade Configuration Manager clients
- Upgrade Configuration Manager consoles
- Re-enable database replicas for management points
- Restore settings for Configuration Manager functionality that you use and that doesn't persist after the upgrade

Scenarios to streamline your installation of System Center Configuration Manager

5/9/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

With the release of update versions for System Center Configuration Manager current branch, there are new scenarios to streamline the install of a new hierarchy to an update version (like update 1610), and to upgrade from Microsoft System Center 2012 Configuration Manager.

Supported scenarios include:

Install a new System Center Configuration Manager current branch hierarchy that runs an update version.

- Install only the top-tier site, and then immediately install an update to bring that site current with the update version that you will use. Then, you can install additional sites directly to that update version.
- In this scenario, you skip the process of installing additional sites to a baseline level, and then updating them to the update version that you want to use.
- In this scenario, you skip the process of installing clients to a baseline version, and then reinstalling them when you update to a later version.

Upgrade a Microsoft System Center 2012 Configuration Manager infrastructure to an update version of System Center Configuration Manager.

- Manually upgrade your central administration site and each primary site to a baseline version (like version 1606) before you install an update version (like version 1610).
- Don't upgrade secondary sites from Microsoft System Center 2012 Configuration Manager until your primary sites run the update version that you will use.
- Don't upgrade clients from Microsoft System Center 2012 Configuration Manager until your primary sites run the update version that you will use.

Scenario: Install a new hierarchy to an update version

In this example scenario, install the first site of a hierarchy by using a baseline version of System Center Configuration Manager, like version 1610. Then, install the 1610 update before you deploy additional sites or clients.

- Because you plan to use an update version (like version 1610) and not remain at a baseline version (like version 1606), you don't need to install additional sites and then upgrade them. This also applies to clients.
- Don't install secondary sites with version 1606 and then upgrade them to version 1610. Instead, install secondary sites after your primary sites run version 1610.

Follow this sequence:

1. **Install a top-level site for your new hierarchy** by using the baseline media.

   - You can use baseline media only to install the first site of a new hierarchy.
   - For example, install a top-level site by using the baseline version of 1606. For more information, see Use the Setup Wizard to install sites.

   After this step, your top-level site runs version 1606.

2. **Use in-console updates to update your top-level site to a later version.**

- Before you install any child sites or clients, update your top-level site to the update version that you plan to use.
- For example, you can update your top-level site that runs version 1606 to version 1610. For more information, see Updates for System Center Configuration Manager.

After this step, your top-level site runs version 1610.

3. **Install new child primary sites below a central administration site.**

   - Use the installation media from the CD.Latest folder on the central administration site server to install child primary sites. For more information, see The CD.Latest folder for System Center Configuration Manager.

     This source media is required to ensure that new child primary sites match the version of the central administration site.

   After this step, your new child primary sites run version 1610.

4. **At each primary site, use the in-console option to install new secondary sites.**

   - Because you did not install secondary sites while primary sites were at version 1606, you do not need to upgrade secondary sites.
   - Instead, install new secondary sites that run version 1610. For more information, see Install a secondary site in the Use the Setup Wizard to install sites topic.

   After this step, new secondary sites are installed and run version 1610.

5. **Install new clients at the primary site.**

   - Because you did not install clients while primary sites were at version 1606, you do not need to upgrade clients from version 1606 to version 1610.
   - Instead, install new clients that run version 1610. For more information, see Deploy clients in System Center Configuration Manager.

   After this step, new clients are installed that run version 1610.

Scenario: Upgrade System Center 2012 Configuration Manager to an update version of System Center Configuration Manager, current branch

In this example scenario, upgrade your Microsoft System Center 2012 Configuration Manager infrastructure to an update version of System Center Configuration Manager, like version 1610.

- The central administration site and each primary site must upgrade to the baseline version 1606 before you install the update for version 1610.
- Secondary sites and clients do not upgrade or install version 1606. Instead, they move directly from Microsoft System Center 2012 Configuration Manager to System Center Configuration Manager version 1610.

Follow this sequence:

1. **Upgrade your top-level Microsoft System Center 2012 Configuration Manager site** to a baseline version of the current branch by using source media for System Center Configuration Manager (like version 1606). For more information, see Upgrade to System Center Configuration Manager.

   - Like traditional upgrade scenarios, you always upgrade the top-level site of a hierarchy first, and then upgrade child sites.

   After this step, your top-level site runs version 1606.

2. **Upgrade each child primary site in your hierarchy** to that same baseline version.

- When you upgrade from Microsoft System Center 2012 Configuration Manager, you must manually upgrade each primary site to a baseline version of the current branch.
- You will not upgrade secondary sites at this point.

After this step, each primary site runs version 1606.

3. **Set maintenance windows on child-primary sites.** After you upgrade all your primary sites to the baseline version, plan to configure maintenance windows to control when those sites install infrastructure updates. For more information, see How to use maintenance windows in System Center Configuration Manager. (Maintenance windows are called *service windows* in version 1606.)

   - A child primary site automatically installs the same updates that you install at a central administration site.
   - Secondary sties do not automatically install new versions. You must upgrade them manually from within the console.

   After this step, when you install updates at the central administration site, child primary sites will only install that update when allowed by their maintenance window.

4. **Install the update version at your top-level site.** This updates your top-level site. After a central administration site installs the update version, each child primary site automatically installs the update unless the installation is blocked by a maintenance window.

   - For example, you can update your top-level site from version 1606 to version 1610. For more information, see Updates for System Center Configuration Manager.

   After this step, your central administration site and each primary site runs version 1610.

5. **Upgrade secondary sites.** After a primary site installs the update and runs version 1610, use the in-console option to upgrade secondary sites.

   - This upgrades secondary sites directly from Microsoft System Center 2012 Configuration Manager to the update version that you installed at the primary site.
   - For information about upgrading a secondary site, see Upgrade sites in the Upgrade to System Center Configuration Manager topic.

6. **Upgrade clients.** To upgrade clients, use the information in How to upgrade clients for Windows computers in System Center Configuration Manager.

   - This upgrades clients directly from Microsoft System Center 2012 Configuration Manager to the update version that you installed at the primary site.

   After this step, clients are upgraded to version 1610 without first upgrading to version 1606.

Uninstall sites and hierarchies in System Center Configuration Manager

5/9/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the following details as a guide if you need to uninstall a System Center Configuration Manager site.

To decommission a hierarchy with multiple sites, the sequence of removal is important. Start by uninstalling the sites at the bottom of the hierarchy and then move upward:

1. Remove secondary sites attached to primary sites.
2. Remove primary sites.
3. After all primary sites are removed, you can uninstall the central administrations site.

Remove a secondary site from a hierarchy

You cannot move a secondary site or reassign a secondary site to a new parent primary site. To be removed from a hierarchy, a secondary site must be deleted from its direct parent site. Use the Delete Secondary Site Wizard from the Configuration Manager console to remove a secondary site. When you remove a secondary site, you must choose whether to delete it or uninstall it:

- **Uninstall the secondary site**. Use this option to remove a functional secondary site that is accessible from the network. This option uninstalls Configuration Manager from the secondary site server, and then deletes all information about the site and its resources from the Configuration Manager site hierarchy. If Configuration Manager installed SQL Server Express as part of the secondary site installation, Configuration Manager will uninstall SQL Express when it uninstalls the secondary site. If SQL Server Express was installed before you installed the secondary site, Configuration Manager will not uninstall SQL Server Express.

- **Delete the secondary site**. Use this option if one of the following is true:

  - A secondary site failed to install
  - The secondary site continues to be displayed in the Configuration Manager console after you uninstall it

  This option deletes all information about the site and its resources from the Configuration Manager hierarchy, but leaves Configuration Manager installed on the secondary site server.

  > **NOTE**
  > You also can use the Hierarchy Maintenance Tool and the **/DELSITE** option to delete a secondary site. For more information, see Hierarchy Maintenance Tool (Preinst.exe) for System Center Configuration Manager.

To uninstall or delete a secondary site

1. Verify that the administrative user that runs Setup has the following security rights:

   - Administrative rights on the secondary site computer
   - Local Administrator rights on the remote site database server for the primary site, if it is remote
   - Infrastructure Administrator or Full Administrator security role on the parent primary site
   - Sysadmin rights on the site database of the secondary site

2. In the Configuration Manager console, select **Administration**.

3. In the **Administration** workspace, expand **Site Configuration**, and then select **Sites**.
4. Select the secondary site server that you want to remove.
5. On the **Home** tab, in the **Site** group, select **Delete**.
6. On the **General** page, select whether to uninstall or delete the secondary site, and then click **Next**.
7. On the **Summary** page, verify the settings, and then select **Next**.
8. On the **Completion** page, select **Close** to exit the wizard.

Uninstall a primary site

You can run Configuration Manager Setup to uninstall a primary site that does not have an associated secondary site. Before you uninstall a primary site, consider the following:

- When Configuration Manager clients are within the boundaries configured at the site, and the primary site is part of a Configuration Manager hierarchy, consider adding the boundaries to a different primary site in the hierarchy before you uninstall the primary site.
- When the primary site server is no longer available, you must use the Hierarchy Maintenance Tool at the central administration site to delete the primary site from the site database. For more information, see Hierarchy Maintenance Tool (Preinst.exe) for System Center Configuration Manager.

Use the following procedure to uninstall a primary site.

To uninstall a primary site

1. Verify that the administrative user that runs Setup has the following security rights:
   - Local Administrator rights on the central administration site server
   - Local Administrator rights on the remote site database server for the central administration site, if it is remote
   - Sysadmin rights on the site database of the central administration site
   - Local Administrator rights on the primary site computer
   - Local Administrator rights on the remote site database server for the primary site, if it is remote
   - A user name associated with the Infrastructure Administrator or Full Administrator security role on the central administration site
2. Start Configuration Manager Setup on the primary site server by using one of the following methods:
   - On **Start**, select **Configuration Manager Setup**.
   - Open Setup.exe from <*ConfigMgrInstallationMedia*>\SMSSETUP\BIN\X64.
   - Open Setup.exe from <*ConfigMgrInstallationPath*>\BIN\X64.
3. On the **Before You Begin** page, select **Next**.
4. On the **Getting Started** page, select **Uninstall a Configuration Manager site**, and then select **Next**.
5. On the **Uninstall the Configuration Manager Site**, specify whether to remove the site database from the primary site server, and whether to remove the Configuration Manager console. By default, Setup removes both items.

   > **IMPORTANT**
   > When a secondary site is attached to the primary site, you must remove the secondary site before you can uninstall the primary site.

6. Select **Yes** to confirm the uninstallation of the Configuration Manager primary site.

Uninstall a primary site that is configured with distributed views

Before you uninstall a child primary site that has distributed views turned on for its replication link to the central administration site, you must turn off distributed views in your hierarchy. Use the following information to turn off distributed views before you uninstall a primary site.

To uninstall a primary site that is configured with distributed views

1. Before you uninstall any primary site, you must turn off distributed views on each link in the hierarchy between the central administration site and a primary site.
2. After you turn off distributed views on each link, confirm that the data from the primary site finishes reinitializing at the central administration site. To monitor the initialization of data, in the Configuration Manager console, in the **Monitoring** workspace, view the link on the **Database Replication** node.
3. After the data successfully reinitializes with the central administration site, you can uninstall the primary site. To uninstall a primary site, see Uninstall a primary site.
4. When the primary site is completely uninstalled, you can reconfigure distributed views on links to primary sites.

> **IMPORTANT**
> If you uninstall the primary site before you turn off distributed views at each site, or before the data from the primary site successfully reinitializes at the central administration site, replication of data between primary sites and the central administration site might fail. In this scenario, you must turn off distributed views for each link in your site hierarchy, and then, after the data successfully reinitializes with the central administration site, you can reconfigure distributed views.

Uninstall the central administration site

You can run Configuration Manager Setup to uninstall a central administration site that does not have child primary sites. Use the following procedure to uninstall the central administration site.

To uninstall a central administration site

1. Verify that the administrative user who runs Setup has the following security rights:
   - Local Administrator rights on the central administration site server
   - Local Administrator rights on the site database server for the central administration site, if the site database server is not installed on the site server
2. Start Configuration Manager Setup on the central administration site server by using one of the following methods:
   - On **Start**, click **Configuration Manager Setup**.
   - Open Setup.exe from <*ConfigMgrInstallationMedia*>\SMSSETUP\BIN\X64.
   - Open Setup.exe from <*ConfigMgrInstallationPath*>\BIN\X64.
3. On the **Before You Begin** page, select **Next**.
4. On the **Getting Started** page, select **Uninstall a Configuration Manager site**, and then select **Next**.
5. On the **Uninstall the Configuration Manager Site**, specify whether to remove the site database from the central administration site server, and whether to remove the Configuration Manager console. By default, Setup removes both items.

> **IMPORTANT**
>
> When there is a primary site attached to the central administration site, you must uninstall the primary site before you can uninstall the central administration site.

6. Select **Yes** to confirm the uninstallation of the Configuration Manager central administration site.

Configure sites and hierarchies for Configuration Manager

8/12/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

After you install your first Configuration Manager site or add additional sites to your hierarchy, use this checklist to ensure that you consider the most common configurations that affect both sites and hierarchies.

The following configuration notes apply to most deployments:

- Some options build upon each other, such as Active Directory Forest Discovery, boundaries, and boundary groups.
- Several configurations have default values to use without configuration changes, at least to start.
- Other configurations, like boundary groups and distribution point groups, require you to configure them before using.

ACTION	DETAILS
Configure role-based administration	Segregate administrative assignments to control which administrative users can view and manage different objects and data in your Configuration Manager environment. Configurations for role-based administration are shared with all sites in a hierarchy. For more information, see Configure role-based administration.
Publish site data to Active Directory Domain Services	Make it easy for clients to find services and efficiently use site resources. First extend the Active Directory schema. Then individually configure each site to publish site data
Configure a service connection point	Plan to install and configure the service connection point at the top-level site of your hierarchy. For more information, see About the service connection point.
Add site system roles	Install one or more additional site system roles for individual sites. For more information, see Add site system roles.
Configure site boundaries and boundary groups	Specify boundaries that define network locations on your intranet that can contain devices that you want to manage. Then configure boundary groups so that clients at those network locations can find Configuration Manager resources. For more information, see Define site boundaries and boundary groups.
Configure distribution point groups	Configure logical groups of distribution points to make managing deployments easier. For more information, see Manage distribution point groups.

ACTION	DETAILS
Run discovery	Run discovery to find resources on your network, including network infrastructure, devices, and users. For more information, see Run discovery.
Add redundancy and capacity for administrators	Install additional SMS Providers and Configuration Manager consoles to expand capacity for administrators to manage your infrastructure: **Install additional SMS providers** to provide redundancy for console and API connections to the site. For more information, see Manage the SMS Provider. **Install additional Configuration Manager consoles** to provide access to additional administrative users. For more information, see Install Configuration Manager consoles.
Configure site components	Configure site components at each site to modify the behavior of site system roles and site status reporting. For more information, see Site components.
Create custom collections	Using information that the site discovers about devices and users, create custom collections of objects to simplify future management tasks. For more information, see How to create collections.
Configure settings to manage high-risk deployments	Configure settings at a site to warn administrators when they create a high-risk deployment. For more information, see Settings to manage high-risk deployments.
Configure database replicas for management points	Configure a database replica to reduce the processor load that's placed on the site database server by management points as they service requests from clients. For more information, see Database replicas for management points.
Configure a SQL Server Always On availability group	Configure availability groups as high-availability and disaster-recovery solutions for hosting the site database at primary sites and the central administration site. For more information, see SQL Server AlwaysOn for a highly available site database.
Modify replication between sites	See Data transfers between sites to learn about the following subjects: Configure file-based replication between secondary sites Configure database replication links Configure distributed views
Configure site servers in passive mode	Starting in version 1806, configure a site server in passive mode for each primary site and the central administration site. This feature provides a highly available site server. For more information, see Site server high availability.

Add site system roles for System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Each System Center Configuration Manager site supports multiple site system roles. Each role extends the functionality and capacity of your site to provide services to the site and to manage devices and users. Each site system role on a site system server must be from the same site.

Configuration Manager does not support site system roles for multiple sites on a single site system server.

> **TIP**
> If you're not familiar with the basics for site system roles or the difference between the site server, site system servers, and site system roles, see Fundamentals of System Center Configuration Manager.

The following topics detail procedures and related details for installing site system roles:

- Install site system roles for System Center Configuration Manager

  This topic provides basic guidance about how to use the two in-console wizards that you can use to install new site system roles.

- Install cloud-based distribution points in Microsoft Azure for System Center Configuration Manager

  When you want to use Microsoft Azure to host content that you deploy to clients, the information in this topic will help you set up the required certificate files to let Configuration Manager communicate with and use your Microsoft Azure subscription. In addition, you will need to set up name resolution to enable your clients to find your cloud-based distribution points.

- Install site system roles for On-premises Mobile Device Management in System Center Configuration Manager

  This topic will help you successfully set up your site system roles to support managing modern devices by using Configuration Manager on-premises MDM.

- Configuration options for site system roles for System Center Configuration Manager

  Some site system roles support configurations that require more details than the user interface can explain. This topic provides those details.

Install site system roles for System Center Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The System Center Configuration Manager console has two wizards you can use to install site system roles:

- **Add Site System Roles Wizard**: Use this wizard to add site system roles to an existing site system server in the site.
- **Create Site System Server Wizard**: Use this wizard to specify a new server as a site system server, and then install one or more site system roles on the server. This wizard is the same as the **Add Site System Roles Wizard**, except that on the first page, you must specify the name of the server to use and the site in which you want to install it.

When you install a site system role on a remote computer (including an instance of the SMS Provider), the computer account of the remote computer is added to a local group on the site server. When the site is installed on a domain controller, the group on the site server is a domain group instead of a local group. In this case, the remote site system role is not operational until either the site system role computer restarts, or the Kerberos ticket for the remote computer's account is refreshed. For more information, see Accounts used in System Center Configuration Manager.

Just prior to installing the site system role, Configuration Manager checks the destination computer to ensure it meets the prerequisites for the site system roles you have selected. Understand the following about installing site system roles:

- By default, when Configuration Manager installs a site system role, the installation files are installed on the first available NTFS formatted disk drive that has the most available free disk space. To prevent Configuration Manager from installing on specific drives, create an empty file named **no_sms_on_drive.sms**. Copy it to the root folder of the drive before you install the site system server.
- Configuration Manager uses the **Site System Installation Account** to install site system roles. You specify this account when you run the applicable wizard to create a new site system server or add site system roles to an existing site system server. By default, this account is the local system account of the site server computer, but you can specify a domain user account for use as the Site System Installation Account. For more information, see Accounts used in System Center Configuration Manager.

To install site system roles on an existing site system server

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Site Configuration**, and click **Servers and Site System Roles**. Then select the server that you want to use for the new site system roles.
3. On the **Home** tab, in the **Server** group, click **Add Site System Roles**.
4. On the **General** page, review the settings, and then click **Next**.

> **TIP**
> To access the site system role from the internet, ensure that you specify an internet fully qualified domain name (FQDN).

5. On the **Proxy** page, specify settings for a proxy server, if site system roles that run on this site system server require a proxy server to connect to locations on the internet. Then click **Next**.
6. On the **System Role Selection** page, select the site system roles that you want to add, and then click **Next**.
7. Complete the wizard.

> **TIP**
> The Windows PowerShell cmdlet, New-CMSiteSystemServer, performs the same function as this procedure. For more information, see New-CMSiteSystemServer in the System Center 2012 Configuration Manager SP1 Cmdlet Reference documentation.

To install site system roles on a new site system server

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Site Configuration**, and click **Servers and Site System Roles**.
3. On the **Home** tab, in the **Create** group, click **Create Site System Server**.
4. On the **General** page, specify the general settings for the site system, and then click **Next**.

> **TIP**
> To access the new site system role from the internet, ensure that you specify an internet FQDN.

5. On the **Proxy** page, specify settings for a proxy server, if site system roles that run on this site system server require a proxy server to connect to locations on the internet. Then click **Next**.
6. On the **System Role Selection** page, select the site system roles that you want to add, and then click **Next**.
7. Complete the wizard.

> **TIP**
> The Windows PowerShell cmdlet, New-CMSiteSystemServer, performs the same function as this procedure. For more information, see New-CMSiteSystemServer in the System Center 2012 Configuration Manager SP1 Cmdlet Reference documentation.

Install a cloud distribution point for Configuration Manager

9/12/2019 • 15 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

> **IMPORTANT**
>
> The implementation for sharing content from Azure has changed. Use a content-enabled cloud management gateway by enabling the option to **Allow CMG to function as a cloud distribution point and serve content from Azure storage**. For more information, see Modify a CMG.
>
> You won't be able to create a traditional cloud distribution point in the future. For more information, see Removed and deprecated features.

This article details the steps to install a Configuration Manager cloud distribution point in Microsoft Azure. It includes the following sections:

Before you begin

Start by reading the article Use a cloud distribution point. That article helps you plan and design your cloud distribution points.

Use the following checklist to make sure you have the necessary information and prerequisites to create a cloud distribution point:

- The site server can connect to Azure. If your network uses a proxy, configure the site system role.
- The **Azure environment** to use. For example, the Azure Public Cloud or the Azure US Government Cloud.
- Starting in version 1806 and *recommended*, use the **Azure Resource Manager deployment**. It has the following requirements:
  - Integration with Azure Active Directory for **Cloud Management**. Azure AD user discovery isn't required.
  - The Azure **Subscription ID**.
  - The Azure **Resource Group**.
  - A **subscription admin account** needs to sign in during the wizard.
- A **server authentication certificate**, exported as a .PFX file.

- A globally unique **service name** for the cloud distribution point.

  > **TIP**
  >
  > Before requesting the server authentication certificate that uses this service name, confirm that the desired Azure domain name is unique. For example, *WallaceFalls.CloudApp.Net*.
  >
  > 1. Sign in to the Azure portal.
  > 2. Select **All resources**, and then select **Add**.
  > 3. Search for **Cloud service**. Select **Create**.
  > 4. In the **DNS name** field, type the prefix you want, for example *WallaceFalls*. The interface reflects whether the domain name is available or already in use by another service.
  >
  > Don't create the service in the portal, just use this process to check the name availability.

- The Azure **region** for this deployment.

- If you still need to use the Azure **classic service deployment** in Configuration Manager version 1810 or earlier, you need the following requirements:

  > **IMPORTANT**
  >
  > Starting in version 1810, classic service deployments in Azure are deprecated in Configuration Manager. Start using Azure Resource Manager deployments for the cloud distribution point. For more information, see Azure Resource Manager.
  >
  > Starting in Configuration Manager version 1902, Azure Resource Manager is the only deployment mechanism for new instances of the cloud distribution point.

  - The Azure **Subscription ID**.
  - An Azure **management certificate**, exported as both .CER and .PFX files. An Azure subscription administrator needs to add the .CER management certificate to the subscription in the Azure portal.

BranchCache

To enable a cloud distribution point to use Windows BranchCache, install the BranchCache feature on the site server.

- If the site server has an on-premises distribution point site system role, configure the option in that role's properties to **Enable and configure BranchCache**. For more information, see Configure a distribution point.
- If the site server doesn't have a distribution point role, install the BranchCache feature in Windows. For more information, see Install the BranchCache feature.

If you've already distributed content to a cloud distribution point, and then decide to enable BranchCache, first install the feature. Then redistribute the content to the cloud distribution point.

> **NOTE**
>
> In Configuration Manager version 1810 and earlier, if you have more than one cloud distribution point, you need to manually set the BranchCache key passphrase. For more information, see Microsoft Support KB 4458143.

Set up

Perform this procedure on the site to host this cloud distribution point as determined by your design.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Cloud Services**, and select **Cloud Distribution Points**. In the ribbon, select **Create Cloud Distribution Point**.
2. On the **General** page of the Create Cloud Distribution Point Wizard, configure the following settings:
   a. First specify the **Azure environment**.
   b. Starting in version 1806 and *recommended*, select **Azure Resource Manager deployment** as the deployment method. Select **Sign in** to authenticate with an Azure subscription admin account. The wizard auto-populates the remaining fields from the information stored during the Azure AD integration prerequisite. If you own multiple subscriptions, select the **Subscription ID** of the desired subscription to use.

> **NOTE**
> Starting in version 1810, classic service deployments in Azure are deprecated in Configuration Manager.
>
> If you need to use a classic service deployment, select that option on this page. First enter your Azure **Subscription ID**. Then select **Browse** and select the .PFX file for the Azure management certificate.

3. Select **Next**. Wait as the site tests the connection to Azure.
4. On the **Settings** page, specify the following settings, and then select **Next**:
   - **Region**: Select the Azure region where you want to create the cloud distribution point.
   - **Resource Group** (Azure Resource Manager deployment method only)
     - **Use existing**: Select an existing resource group from the drop-down list.
     - **Create new**: Enter the new resource group name to create in your Azure subscription.
   - **Primary site**: Select the primary site to distribute content to this distribution point.
   - **Certificate file**: Select **Browse** and select the .PFX file for this cloud distribution point's server authentication certificate. The common name from this certificate populates the required **Service FQDN** and **Service name** fields.

> **NOTE**
> The cloud distribution point server authentication certificate supports wildcards. If you use a wildcard certificate, replace the asterisk (`*`) in the **Service FQDN** field with the desired hostname for the service.

5. On the **Alerts** page, set up storage quotas, transfer quotas, and at what percentage of these quotas you want Configuration Manager to generate alerts. Then select **Next**.
6. Complete the wizard.

Monitor installation

The site starts to create a new hosted service for the cloud distribution point. After you close the wizard, monitor the installation progress of the cloud distribution point in the Configuration Manager console. Also monitor the **CloudMgr.log** file on the primary site server. If necessary, monitor the provisioning of the cloud service in the Azure portal.

> **NOTE**
>
> It can take up to 30 minutes to provision a new distribution point in Azure. The **CloudMgr.log** file repeats the following message until the storage account is provisioned:
>
> `Waiting for check if container exists. Will check again in 10 seconds`
>
> After it provisions the storage account, the service is created and configured.

Verify installation

Verify that the cloud distribution point installation is complete by using the following methods:

- In the Configuration Manager console, go to the **Administration** workspace. Expand **Cloud Services**, and select the **Cloud Distribution Points** node. Find the new cloud distribution point in the list. The Status column should be **Ready**.
- In the Configuration Manager console, go to the **Monitoring** workspace. Expand **System Status**, and select the **Component Status** node. Show all messages from the **SMS_CLOUD_SERVICES_MANAGER** component, and look for status message ID **9409**.
- If necessary, go to the Azure portal. The **Deployment** for the cloud distribution point displays a status of **Ready**.

Configure DNS

Before clients can use the cloud distribution point, they must be able to resolve the name of the cloud distribution point to an IP address that Azure manages. The management point gives them the **Service FQDN** of the cloud distribution point. The cloud distribution point exists in Azure as the **Service name**. See these values on the **Settings** tab of the cloud distribution point properties.

> **NOTE**
>
> The **Cloud Distribution Points** node in the console includes a column named **Service Name**, but actually shows the **Service FQDN** value. To see both values, open **Properties** for the cloud distribution point and switch to the **Settings** tab.

The server authentication certificate common name should include your domain name. This name is required when you purchase a certificate from a public provider. It's recommended when issuing this certificate from your PKI. For example, `WallaceFalls.contoso.com`. When you specify this certificate in the Create Cloud Distribution Point Wizard, the common name populates the **Service FQDN** property (`WallaceFalls.contoso.com`). The **Service name** takes the same hostname (`WallaceFalls`) and appends it to the Azure domain name, `cloudapp.net`. In this scenario, clients need to resolve your domain's **Service FQDN** (`WallaceFalls.contoso.com`) to the Azure **Service name** (`WallaceFalls.cloudapp.net`). Create a CNAME alias to map these names.

Create CNAME alias

Create a canonical name record (CNAME) in your organization's public, internet-facing DNS. This record creates an alias for the cloud distribution point's **Service FQDN** property that clients receive, to the Azure **Service name**. For example, create a new CNAME record for `WallaceFalls.contoso.com` to `WallaceFalls.cloudapp.net`.

Client name resolution process

The following process shows how a client resolves the name of the cloud distribution point:

1. The client gets the **Service FQDN** of the cloud distribution point in the list of content sources. For example, `WallaceFalls.contoso.com`.
2. It queries DNS, which resolves the Service FQDN using the CNAME alias to the Azure **Service name**. For example, `WallaceFalls.cloudapp.net`.

3. It queries DNS again, which resolves the Azure service name to the Azure public IP address.
4. The client uses this IP address to start communication with the cloud distribution point.
5. The cloud distribution point presents the server authentication certificate to the client. The client uses the trust chain of the certificate to validate.

Set up site server proxy

The primary site server that manages the cloud distribution point needs to communicate with Azure. If your organization uses a proxy server to control internet access, configure the primary site server to use this proxy.

For more information, see Proxy server support.

Distribute content and configure clients

Distribute content to the cloud distribution point the same as any other on-premises distribution point. The management point doesn't include the cloud distribution point in the list of content locations unless it has the content that clients request. For more information, see Distribute and manage content.

Manage a cloud distribution point the same as any other on-premises distribution point. These actions include assigning it to a distribution point group, and managing content packages. For more information, see Install and configure distribution points.

Default client settings automatically enable clients to use cloud distribution points. Control access to all cloud distribution points in your hierarchy with the following client setting:

- In the **Cloud Settings** group, modify the setting **Allow access to cloud distribution points**.
  - By default, this setting is set to **Yes**.
  - Modify and deploy this setting for both users and devices.

Manage and monitor

Monitor content that you distribute to a cloud distribution point the same as with any other on-premises distribution points. For more information, see Monitor content.

Alerts

Configuration Manager periodically checks the Azure service. If the service isn't active, or if there are subscription or certificate issues, Configuration Manager raises an alert.

Configure thresholds for the amount of data that you want to store on the cloud distribution point, and for the amount of data that clients download from the distribution point. Use alerts for these thresholds to help you decide when to stop or delete the cloud service, adjust the content that you store on the cloud distribution point, or modify which clients can use the service.

- **Storage alert threshold**: The storage alert threshold sets an upper limit in GB on the amount of data or content that you want store on the cloud distribution point. By default, this threshold is 2,000 GB. Configuration Manager generates warning and critical alerts when the remaining free space reaches the levels that you specify. By default, these alerts occur at 50% and 90% of the threshold.
- **Monthly transfer alert threshold**: The monthly transfer alert threshold helps you to monitor the amount of content that transfers from the distribution point to clients for a 30-day period. By default, this threshold is 10,000 GB. The site raises warning and critical alerts when transfers reach values that you define. By default, these alerts occur at 50% and 90% of the threshold.

> **IMPORTANT**
> Configuration Manager monitors the transfer of data, but does not stop the transfer of data beyond the specified transfer alert threshold.

Specify thresholds for each cloud distribution point during installation, or use the **Alerts** tab of the cloud distribution point properties.

> **NOTE**
> Alerts for a cloud distribution point depend on usage statistics from Azure, which can take up to 24 hours to become available. For more information about Storage Analytics for Azure, see Storage Analytics.

In an hourly cycle, the primary site that monitors the cloud distribution point downloads transaction data from Azure. It stores this transaction data in the `CloudDP-<ServiceName>.log` file on the site server. Configuration Manager then evaluates this information against the storage and transfer quotas for each cloud distribution point. When the transfer of data reaches or exceeds the specified volume for either warnings or critical alerts, Configuration Manager generates the appropriate alert.

> **WARNING**
> Because the site downloads information about data transfers from Azure every hour, the usage might exceed a warning or critical threshold before Configuration Manager can access the data and raise an alert.

Modify

View high-level information about the distribution point in the **Cloud Distribution Points** node under **Cloud Services** in the **Administration** workspace of the Configuration Manager console. Select a distribution point and select **Properties** to see more details.

When you edit the properties of a cloud distribution point, the following tabs include settings to edit:

Settings

- **Description**
- **Certificate file**: Before the server authentication certificate expires, issue a new certificate with the same common name. Then add the new certificate here for the service to start using. If the certificate expires, clients won't trust and use the service.

Alerts

Adjust the data thresholds for storage and monthly transfer alerts.

Content

Manage content the same as for an on-premises distribution point.

Redeploy the service

More significant changes, such as the following configurations, require redeploying the service:

- Classic deployment method to Azure Resource Manager
- Subscription
- Service name
- Private to public PKI
- Azure region

Starting in version 1806, if you have an existing cloud distribution point on the classic deployment method, in order to use the Azure Resource Manager deployment method you need to deploy a new cloud distribution point. There are two options:

- If you want to reuse the same service name:
  1. First delete the classic cloud distribution point. If there isn't another cloud distribution point, then clients may not be able to get content.
  2. Create a new cloud distribution point using a Resource Manager deployment. Reuse the same server authentication certificate.
  3. Distribute the necessary software package content to the new cloud distribution point.
- If you want to use a new service name:
  1. Create a new cloud distribution point using a Resource Manager deployment. Use a new server authentication certificate.
  2. Distribute the necessary software package content to the new cloud distribution point.
  3. Delete the classic cloud distribution point.

> **TIP**
> To determine the current deployment model of a cloud distribution point:
>
> 1. In the Configuration Manager console, go to the **Administration** workspace, expand **Cloud Services**, and select the **Cloud Distribution Points** node.
> 2. Add the **Deployment Model** attribute as a column to the list view. For a Resource Manager deployment, this attribute is **Azure Resource Manager**.

Stop or start the cloud service on demand

Stop a cloud distribution point at any time in the Configuration Manager console. This action immediately prevents clients from downloading additional content from the service. Restart the cloud service from the Configuration Manager console to restore access for clients. For example, stop a cloud service when it reaches a data threshold.

When you stop a cloud distribution point, the cloud service doesn't delete the content from the storage account. It also doesn't prevent the site server from transferring additional content to the cloud distribution point. The management point still returns the cloud distribution point to clients as a valid content source.

Use the following procedure to stop a cloud distribution point:

1. In the Configuration Manager console, go to the **Administration** workspace. Expand **Cloud Services**, and select the **Cloud Distribution Points** node.
2. Select the cloud distribution point. To stop the cloud service that runs in Azure, select **Stop service** in the ribbon.
3. Select **Start service** to restart the cloud distribution point.

Delete a cloud distribution point

To uninstall a cloud distribution point, select the distribution point in the Configuration Manager console, and then select **Delete**.

When you delete a cloud distribution point from a hierarchy, Configuration Manager removes the content from the cloud service in Azure.

Manually removing any components in Azure causes the system to be inconsistent. This state leaves orphaned

information, and unexpected behaviors may occur.

Advanced troubleshooting

If you need to collect diagnostic logging from the Azure VMs to help troubleshoot problems with your cloud distribution point, use the following PowerShell sample to enable the service diagnostic extension for the subscription:

```
# Change these variables for your Azure environment. The current values are provided as examples. You can find
the values for these from the Azure portal.
$storage_name="4780E3836835850223C071" # The name of the storage account that goes with the CloudDP
$key="3jSyvMssuTyAyj5jWHKtf2bV5JF^aDN%z%2g*RImGK8R4vcu3PE07!P7CKTbZhT1Sxd3l^t69R8Cpsdl1xhlhZtl" # The storage
access key from the Storage Account view
$service_name="4780E3836835850223C071" # The name of the cloud service for the CloudDP, which for a Cloud DP
is the same as the storage name
$azureSubscriptionName="8ba1cb83-84a2-457e-bd37-f78d2dd371ee" # The subscription name the tenant is using
$subscriptionId="8ba1cb83-84a2-457e-bd37-f78d2dd371ee" # The subscription ID the tenant is using

# This variable is the path to the config file on the local computer.
$public_config="F:\PowerShellDiagFile\diagnostics.wadcfgx"

# These variables are for the Azure management certificate. Install it in the Current User certificate store
on the system running this script.
$thumbprint="dac9024f54d8f6df94935fb1732638ca6ad77c13" # The thumbprint of the Azure management certificate
$mycert = Get-Item cert:\\CurrentUser\My\$thumbprint

Set-AzureSubscription -SubscriptionName $azureSubscriptionName -SubscriptionId $subscriptionId -Certificate
$mycert

Select-AzureSubscription $azureSubscriptionName

Set-AzureServiceDiagnosticsExtension -StorageAccountName $storage_name -StorageAccountKey $key -
DiagnosticsConfigurationPath $public_config –ServiceName $service_name -Slot 'Production' -Verbose
```

The following sample is an example **diagnostics.wadcfgx** file as referenced in the **public_config** variable in the above PowerShell script. For more information, see Azure Diagnostics extension configuration schema.

```
<?xml version="1.0" encoding="utf-8"?>
<PublicConfig xmlns="http://schemas.microsoft.com/ServiceHosting/2010/10/DiagnosticsConfiguration">
  <WadCfg>
    <DiagnosticMonitorConfiguration overallQuotaInMB="4096">
      <Directories scheduledTransferPeriod="PT1M">
        <IISLogs containerName ="wad-iis-logfiles" />
        <FailedRequestLogs containerName ="wad-failedrequestlogs" />
      </Directories>
      <WindowsEventLog scheduledTransferPeriod="PT1M">
        <DataSource name="Application!*" />
      </WindowsEventLog>
      <Logs scheduledTransferPeriod="PT1M" scheduledTransferLogLevelFilter="Information" />
      <CrashDumps dumpType="Full">
        <CrashDumpConfiguration processName="WaAppAgent.exe" />
        <CrashDumpConfiguration processName="WaIISHost.exe" />
        <CrashDumpConfiguration processName="WindowsAzureGuestAgent.exe" />
        <CrashDumpConfiguration processName="WaWorkerHost.exe" />
        <CrashDumpConfiguration processName="DiagnosticsAgent.exe" />
        <CrashDumpConfiguration processName="w3wp.exe" />
      </CrashDumps>
      <PerformanceCounters scheduledTransferPeriod="PT1M">
        <PerformanceCounterConfiguration counterSpecifier="\Memory\Available MBytes" sampleRate="PT3M" />
        <PerformanceCounterConfiguration counterSpecifier="\Web Service(_Total)\ISAPI Extension Requests/sec"
sampleRate="PT3M" />
        <PerformanceCounterConfiguration counterSpecifier="\Web Service(_Total)\Bytes Total/Sec"
sampleRate="PT3M" />
        <PerformanceCounterConfiguration counterSpecifier="\ASP.NET Applications(__Total__)\Requests/Sec"
sampleRate="PT3M" />
        <PerformanceCounterConfiguration counterSpecifier="\ASP.NET Applications(__Total__)\Errors Total/Sec"
sampleRate="PT3M" />
        <PerformanceCounterConfiguration counterSpecifier="\ASP.NET\Requests Queued" sampleRate="PT3M" />
        <PerformanceCounterConfiguration counterSpecifier="\ASP.NET\Requests Rejected" sampleRate="PT3M" />
        <PerformanceCounterConfiguration counterSpecifier="\Processor(_Total)\% Processor Time"
sampleRate="PT3M" />
      </PerformanceCounters>
    </DiagnosticMonitorConfiguration>
  </WadCfg>
</PublicConfig>
```

About the service connection point in Configuration Manager

6/20/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The service connection point is a site system role that serves several important functions for the hierarchy. Before you set up the service connection point, understand and plan for its range of uses. Planning for usage might affect how you set up this site system role:

- **Manage mobile devices with Microsoft Intune**: This role replaces the Windows Intune connector that previous versions of Configuration Manager used and can be configured with your Intune subscription details. For more information, see Hybrid mobile device management (MDM).
- **Manage mobile devices with on-premises MDM**: This role provides support for on-premises devices that you manage and that don't connect to the internet. For more information, see Manage mobile devices with on-premises infrastructure.
- **Upload usage data from your Configuration Manager infrastructure**: You can control the level or amount of detail that you upload. Uploaded data helps:
  - Proactively identify and troubleshoot problems
  - Improve our products and service
  - Identify updates for Configuration Manager that apply to the version of Configuration Manager that you use

  For more information about data that each level collects and how to change the collection level after the role installs, see Diagnostics and usage data. Then follow the link for the version of Configuration Manager that you use.

  For more information, see Usage data levels and settings.
- **Download updates that apply to your Configuration Manager infrastructure**: Only relevant updates for your infrastructure are made available based on usage data you upload.
- **Each hierarchy supports a single instance of this role**:
  - The site system role can only be installed at the top-tier site of your hierarchy, which is a central administration site or stand-alone primary site.
  - If you expand a stand-alone primary site to a larger hierarchy, you must uninstall this role from the primary site and can then install it at the central administration site.

Modes of operation

The service connection point supports two modes of operation:

- In **online mode**, the service connection point automatically checks every 24 hours for updates. It downloads new updates that are available for your current infrastructure and product version to make them available in the Configuration Manager console.
- In **offline mode**, the service connection point doesn't connect to the Microsoft cloud service. To manually

import available updates, use the service connection tool.

If you change between online or offline modes after you install the service connection point, you must restart the SMS_DMP_DOWNLOADER thread of the Configuration Manager SMS_Executive service before the change becomes effective. You can use the Configuration Manager Service Manager to restart only the SMS_DMP_DOWNLOADER thread of the SMS_Executive service. You can also restart the SMS_Executive service for Configuration Manager, which restarts most site components. Alternatively, you can wait for a scheduled task like a site backup, which stops and then later restarts the SMS_Executive service for you.

To use the Configuration Manager Service Manager, in the console go to **Monitoring** > **System Status** > **Component Status**, choose **Start**, and then choose **Configuration Manager Service Manager**. In the service manager:

- In the navigation pane, expand the site, expand **Components**, and then choose the component that you want to restart.
- In the details pane, right-click the component, and then choose **Query**.
- After the status of the component is confirmed, right-click the component again, and then choose **Stop**.
- **Query** the component again to confirm that it is stopped. Right-click the component one more time, and then choose **Start**.

> **IMPORTANT**
> The process that adds a Microsoft Intune subscription to the service connection point automatically sets the site system role to be online. The service connection point doesn't support offline mode when it's set up with an Intune subscription.

When the role installs on a computer that is remote from the site server:

- The computer account of the site server must be a local admin on the computer that hosts a remote service connection.
- You must set up the site system server that hosts the role with a site system installation account.
- The distribution manager on the site server uses the site system installation account to transfer updates from the service connection point.

Internet access requirements

If your organization restricts network communication with the internet using a firewall or proxy device, you need to allow the service connection point to access internet endpoints.

For more information, see Internet access requirements.

Install the service connection point

When you run **Setup** to install the top-tier site of a hierarchy, you have the option to install the service connection point.

After setup runs, or if you are reinstalling the site system role, use the **Add Site System Roles** wizard or the **Create Site System Server** wizard to install the site system on a server at the top-tier site of your hierarchy, that is, the central administration site or a stand-alone primary site. Both wizards are on the **Home** tab in the console at **Administration** > **Site Configuration** > **Servers and Site System Roles**.

Log files used by the service connection point

To view information about uploads to Microsoft, view the **Dmpuploader.log** on the computer that runs the service connection point. For downloads, including download progress of updates, view **Dmpdownloader.log**. For the complete list of logs related to the service connection point, see Service connection point in the Configuration Manager log files article.

You can also use the following flowcharts to understand the process flow and key log entries for update downloads and replication of updates to other sites:

- Flowchart - Download updates
- Flowchart - Update replication

Configuration options for site system roles in Configuration Manager

8/30/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Most configuration options for Configuration Manager site system roles are self-explanatory or are explained in the wizard or dialog boxes when you configure them. The following sections explain site system roles whose settings might require additional information.

Application catalog website point

> **IMPORTANT**
>
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features

For more information about how to set up the application catalog website point, see Plan for and configure application management.

Application catalog web service point

> **IMPORTANT**
>
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features

For more information about how to set up the Application Catalog web service point, see Plan for and configure application management.

Certificate registration point

For more information about how to set up the certificate registration point, see Introduction to certificate profiles.

Distribution point

For more information about how to set up the distribution point for content deployment, see Manage content and content infrastructure.

For more information about how to set up the distribution point for PXE deployments, see Use PXE to deploy Windows over the network.

For more information about how to set up the distribution point for multicast deployments, see Use multicast to deploy Windows over the network.

Install and configure IIS if required by Configuration Manager

Select this option to let Configuration Manager install and set up IIS on the site system if it's not already installed. IIS must be installed on all distribution points, and you must select this setting to continue in the wizard.

Site system installation account

For distribution points that are installed on a site server, only the computer account of the site server is supported for use as the site system installation account. For more information, see Accounts.

Enrollment point

Enrollment points are used to install macOS computers and enroll devices that you manage with on-premises mobile device management. For more information, see the following articles:

- How to deploy clients to Macs
- How users enroll devices with on-premises MDM

Allowed connections

The HTTPS setting is automatically selected and requires a PKI certificate on the server for server authentication to the enrollment proxy point, and encryption of data over SSL. For more information, see PKI certificate requirements.

For an example deployment of the server certificate and information about how to configure it in IIS, see Deploying the web server certificate for site systems that run IIS .

Enrollment proxy point

For more information about how to set up an enrollment proxy point for mobile devices, see How users enroll devices with on-premises MDM.

Client connections

The HTTPS setting is automatically selected. It requires the following PKI certificates on the server:

- For server authentication to mobile devices and Mac computers that you enroll with Configuration Manager
- For encryption of data over Secure Sockets Layer (SSL)

For more information about the certificate requirements, see PKI certificate requirements.

For an example deployment of the server certificate and information about how to configure it in IIS, see Deploying the web server certificate for site systems that run IIS .

Fallback status point

Number of state messages and Throttle interval (in seconds)

The default settings for these options are 10,000 state messages and 3,600 seconds for the throttle interval. While these settings are sufficient for most circumstances, you might have to change them when both of the following conditions are true:

- The fallback status point accepts connections only from the intranet.
- You use the fallback status point during a client deployment rollout for many computers.

In this scenario, a continuous stream of state messages might create a backlog of state messages that causes high processor usage on the site server for a sustained period. In addition, you might not see up-to-date information about the client deployment in the Configuration Manager console and in the client deployment reports.

These fallback status point settings are designed to be set up for state messages that are generated during client deployment. The settings aren't designed to be set up for client communication issues, like when clients on the internet can't connect to their internet-based management point. Because the fallback status point can't apply these settings just to the state messages that are generated during client deployment, don't configure these settings when the fallback status point accepts connections from the internet.

Each computer that successfully installs the Configuration Manager client sends the following four state messages to the fallback status point:

- Client deployment started
- Client deployment succeeded
- Client assignment started
- Client assignment succeeded

Computers that can't be installed or that assign the Configuration Manager client send additional state messages.

For example, if you deploy the Configuration Manager client to 20,000 computers, the deployment might send 80,000 state messages to the fallback status point. Because the default throttling configuration lets 10,000 state messages to be sent to the fallback status point each 3,600 seconds (1 hour), state messages might become backlogged on the fallback status point. Also consider the available network bandwidth between the fallback status point and the site server and the processing power of the site server to process many state messages.

To help prevent these issues, consider an increase in the number of state messages and a decrease in the throttle interval.

Reset the throttle values for the fallback status point if either of the following conditions is true:

- You calculate that the current throttle values are higher than required to process state messages from the fallback status point.
- You find that the current throttle settings create high processor usage on the site server.

Don't change the settings for the fallback status point throttle settings unless you understand the consequences. For example, when you increase the throttle settings to high, the processor usage on the site server can increase to high, which slows down all site operations.

Database replicas for management points for System Center Configuration Manager

9/11/2019 • 23 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

System Center Configuration Manager primary sites can use a database replica to reduce the CPU load placed on the site database server by management points as they service requests from clients.

- When a management point uses a database replica, that management point requests data from the SQL Server computer that hosts the database replica instead of from the site database server.
- This can help reduce the CPU processing requirements on the site database server by offloading frequent processing tasks related to clients. An example of frequent processing tasks for clients includes sites where there are a large numbers of clients that make frequent requests for client policy

Prepare to use database replicas

About database replicas for management points:

- Replicas are a partial copy of the site database that is replicated to a separate instance of SQL Server:
  - Primary sites support a dedicated database replica for each management point at the site (Secondary sites do not support database replicas)
  - A single database replica can be used by more than a one management point from the same site
  - A SQL server can host multiple database replicas for use by different management points so long as each runs in a separate instance of SQL Server
- Replicas synchronize a copy of the site database on a fixed schedule from data that is published by the sites database server for this purpose.
- Management points can be configured to use a replica when you install the management point, or at a later time by reconfiguring the previously installed management point to use the database replica
- Regularly monitor the site database server and each database replica server to ensure that replication occurs between them, and that the performance of the database replica server is sufficient for the site and client performance that you require

Prerequisites for database replicas:

- **SQL Server requirements:**
  - The SQL Server that hosts the database replica must meet the same requirements as the site database server. However, the replica server does not need to run the same version or edition of SQL Server as the site database server, as long as it runs a supported version and edition of SQL Server. For information see Support for SQL Server versions for System Center Configuration Manager
  - The SQL Server Service on the computer that hosts the replica database must run as the **System** account.
  - Both the SQL Server that hosts the site database and that hosts a database replica must have **SQL Server replication** installed.

- The site database must **publish** the database replica, and each remote database replica server must **subscribe** to the published data.
- Both the SQL Server that hosts the site database and that hosts a database replica must be configured to support a **Max Text Repl Size** of 2 GB. For an example of how to configure this for SQL Server 2012, see Configure the max text repl size Server Configuration Option.

- **Self-signed certificate:** To configure a database replica, you must create a self-signed certificate on the database replica server and make this certificate available to each management point that will use that database replica server.
  - The certificate is automatically available to a management point that is installed on the database replica server.
  - To make this certificate available to remote management points, you must export the certificate and then add it to the **Trusted People** certificate store on the remote management point.
- **Client notification:** To support client notification with a database replica for a management point, you must configure communication between the site database server and the database replica server for the **SQL Server Service Broker**. This requires you to:
  - Configure each database with information about the other database
  - Exchange certificates between the two databases for secure communication

Limitations when you use database replicas:

- When your site is configured to publish database replicas, the following procedures should be used in place of normal guidance:
  - Uninstall a site server that publishes a database replica
  - Move a site server database that publishes a database replica
- **Upgrades to System Center Configuration Manager**: Before you upgrade a site, either from System Center 2012 Configuration Manager to System Center Configuration Manager Current Branch or updating Configuration Manager Current Branch to the latest release, you must disable database replicas for management points. After your site upgrades, you can reconfigure the database replicas for management points.
- **Multiple replicas on a single SQL Server:** If you configure a database replica server to host multiple database replicas for management points (each replica must be on a separate instance) you must use a modified configuration script (from Step 4 of the following section) to prevent overwriting the self-signed certificate in use by previously configured database replicas on that server.

Configure database replicas

To use configure a database replica, the following steps are required:

- Step 1 - Configure the site database server to Publish the database replica
- Step 2 - Configuring the database replica server
- Step 3 - Configure management points to use the database replica
- Step 4 -Configure a self-signed certificate for the database replica server
- Step 5 - Configure the SQL Server Service Broker for the database replica server

Step 1 - Configure the site database server to Publish the database replica

Use the following procedure as an example of how to configure the site database server on a Windows Server 2008 R2 computer to publish the database replica. If you have a different operating system version, refer to your operating system documentation and adjust the steps in this procedure as necessary.

To configure the site database server

1. On the site database server, set the SQL Server Agent to automatically start.
2. On the site database server, create a local user group with the name **ConfigMgr_MPReplicaAccess**. You must add the computer account for each database replica server that you use at this site to this group to enable those database replica servers to synchronize with the published database replica.
3. On the site database server, configure a file share with the name **ConfigMgr_MPReplica**.
4. Add the following permissions to the **ConfigMgr_MPReplica** share:

   > **NOTE**
   > If the SQL Server Agent uses an account other than the local system account, replace SYSTEM with that account name in the following list.

   - **Share Permissions**:
     - SYSTEM: **Write**
     - ConfigMgr_MPReplicaAccess: **Read**
   - **NTFS Permissions**:
     - SYSTEM: **Full Control**
     - ConfigMgr_MPReplicaAccess: **Read**, **Read & execute**, **List folder contents**
5. Use **SQL Server Management Studio** to connect to the site database and run the following stored procedure as a query: **spCreateMPReplicaPublication**

When the stored procedure completes, the site database server is configured to publish the database replica.

Step 2 - Configuring the database replica server

The database replica server is a computer that runs SQL Server and that hosts a replica of the site database for management points to use. On a fixed schedule, the database replica server synchronizes its copy of the database with the database replica that is published by the site database server.

The database replica server must meet the same requirements as the site database server. However, the database replica server can run a different edition or version of SQL Server than the site database server uses. For information about the supported versions of SQL Server, see the Support for SQL Server versions for System Center Configuration Manager topic.

> **IMPORTANT**
> The SQL Server Service on the computer that hosts the replica database must run as the System account.

Use the following procedure as an example of how to configure a database replica server on a Windows Server 2008 R2 computer. If you have a different operating system version, refer to your operating system documentation and adjust the steps in this procedure as necessary.

To configure the database replica server

1. On the database replica server, set the SQL Server Agent to automatic startup.
2. On the database replica server, use **SQL Server Management Studio** to connect to the local server,

browse to the **Replication** folder, click Local Subscriptions, and select **New Subscriptions** to start the **New Subscription Wizard**:

a. On the **Publication** page, in the **Publisher** list box, select **Find SQL Server Publisher**, enter the name of the sites database server, and then click **Connect**.

b. Select **ConfigMgr_MPReplica**, and then click **Next**.

c. On the **Distribution Agent Location** page, select **Run each agent at its Subscriber (pull subscriptions)**, and click **Next**.

d. On the **Subscribers** page do one of the following:

- Select an existing database from the database replica server to use for the database replica, and then click **OK**.
- Select **New database** to create a new database for the database replica. On the **New Database** page, specify a database name, and then click **OK**.

e. Click **Next** to continue.

f. On the **Distribution Agent Security** page, click the properties button **(....)** in the Subscriber Connection row of the dialog box, and then configure the security settings for the connection.

> **TIP**
> The properties button, **(....)**, is in the fourth column of the display box.

Security settings:

- Configure the account that runs the Distribution Agent process (the process account):
  - If the SQL Server Agent runs as local system, select **Run under the SQL Server Agent service account (This is not a recommended security best practice.)**
  - If the SQL Server Agent runs by using a different account, select **Run under the following Windows account**, and then configure that account. You can specify a Windows account or a SQL Server account.

> **IMPORTANT**
> You must grant the account that runs the Distribution Agent permissions to the publisher as a pull subscription. For information about configuring these permissions, see Distribution Agent Security in the SQL Server TechNet Library.

- For **Connect to the Distributor**, select **By impersonating the process account**.
- For **Connect to the Subscriber**, select **By impersonating the process account**.

  After you configure the connection security settings, click **OK** to save them, and then click **Next**.

g. On the **Synchronization Schedule** page, in the **Agent Schedule** list box, select **Define schedule**, and then configure the **New Job Schedule**. Set the frequency to occur **Daily**, recur every **5 minute(s)**, and the duration to have **No end date**. Click **Next** to save the schedule, and then click **Next** again.

h. On the **Wizard Actions** page, select the check box for **Create the subscriptions(s)**, and then click

Next.

i. On the **Complete the Wizard** page, click **Finish**, and then click **Close** to complete the Wizard.

3. Immediately after completing the New Subscription Wizard, use **SQL Server Management Studio** to connect to the database replica server database and run the following query to enable the TRUSTWORTHY database property: `ALTER DATABASE <MP Replica Database Name> SET TRUSTWORTHY ON;`

4. Review the synchronization status to validate that the subscription is successful:

   - On the subscriber computer:
     - In **SQL Server Management Studio**, connect to the database replica server and expand **Replication**.
     - Expand **Local Subscriptions**, right-click the subscription to the site database publication, and then select **View Synchronization Status**.
   - On the publisher computer:
     - In **SQL Server Management Studio**, connect to the site database computer, right-click the **Replication** folder, and then select **Launch Replication Monitor**.

5. To enable common language runtime (CLR) integration for the database replica, use **SQL Server Management Studio** to connect to the database replica on the database replica server, and run the following stored procedure as a query: **exec sp_configure 'clr enabled', 1; RECONFIGURE WITH OVERRIDE**

6. For each management point that uses a database replica server, add that management points computer account to the local **Administrators** group on that database replica server.

   > **TIP**
   > This step is not necessary for a management point that runs on the database replica server.

   The database replica is now ready for a management point to use.

Step 3 - Configure management points to use the database replica

You can configure a management point at a primary site to use a database replica when you install the management point role, or you can reconfigure an existing management point to use a database replica.

Use the following information to configure a management point to use a database replica:

- **To configure a new management point:** On the **Management Point Database** page of the wizard that you use to install the management point, select **Use a database replica**, and specify the FQDN of the computer that hosts the database replica. Next, for **ConfigMgr site database name**, specify the database name of the database replica on that computer.
- **To configure a previously installed management point**: Open the properties page of the management point, select the **Management Point Database** tab, select **Use a database replica**, and then specify the FQDN of the computer that hosts the database replica. Next, for **ConfigMgr site database name**, specify the database name of the database replica on that computer.
- **For each management point that uses a database replica**, you must manually add the computer account of the management point server to the **db_datareader** role for the database replica.

In addition to configuring the management point to use the database replica server, you must enable **Windows Authentication** in **IIS** on the management point:

1. Open **Internet Information Services (IIS) Manager**.
2. Select the website used by the management point, and open **Authentication**.
3. Set **Windows Authentication** to **Enabled**, and then close **Internet Information Services (IIS) Manager**.

Step 4 -Configure a self-signed certificate for the database replica server

You must create a self-signed certificate on the database replica server and make this certificate available to each management point that will use that database replica server.

The certificate is automatically available to a management point that is installed on the database replica server. However, to make this certificate available to remote management points, you must export the certificate and then add it to the Trusted People certificate store on the remote management point.

Use the following procedures as an example of how to configure the self-signed certificate on the database replica server for a Windows Server 2008 R2 computer. If you have a different operating system version, refer to your operating system documentation and adjust the steps in these procedures as necessary.

To configure a self-signed certificate for the database replica server

1. On the database replica server, open a PowerShell command prompt with administrative privileges, and then run the following command: **set-executionpolicy UnRestricted**
2. Copy the following PowerShell script and save it as a file with the name **CreateMPReplicaCert.ps1**. Place a copy of this file in the root folder of the system partition of the database replica server.

> **IMPORTANT**
> If you are configuring more than one database replica on a single SQL Server, for each subsequent replica you configure you must use a modified version of this script for this procedure. See Supplemental script for additional database replicas on a single SQL Server

```
# Script for creating a self-signed certificate for the local machine and configuring SQL Server to use
it.

Param($SQLInstance)

$ConfigMgrCertFriendlyName = "ConfigMgr SQL Server Identification Certificate"

# Get local computer name
$computerName = "$env:computername"

# Get the sql server name
#$key="HKLM:\SOFTWARE\Microsoft\SMS\MP"
#$value="SQL Server Name"
#$sqlServerName= (Get-ItemProperty $key).$value
#$dbValue="Database Name"
#$sqlInstance_DB_Name= (Get-ItemProperty $key).$dbValue

$sqlServerName = [System.Net.Dns]::GetHostByName("localhost").HostName
$sqlInstanceName = "MSSQLSERVER"
$SQLServiceName = "MSSQLSERVER"

if ($SQLInstance -ne $Null)
{
    $sqlInstanceName = $SQLInstance
    $SQLServiceName = "MSSQL$" + $SQLInstance
}

# Delete existing cert if one exists
function Get-Certificate($storename, $storelocation)
{
```

```
    $store=new-object System.Security.Cryptography.X509Certificates.X509Store($storename,$storelocation)
    $store.Open([Security.Cryptography.X509Certificates.OpenFlags]::ReadWrite)
    $store.Certificates
}

$cert = Get-Certificate "My" "LocalMachine" | ?{$_.FriendlyName -eq $ConfigMgrCertFriendlyName}
if($cert -is [Object])
{
    $store = new-object System.Security.Cryptography.X509Certificates.X509Store("My","LocalMachine")
    $store.Open([Security.Cryptography.X509Certificates.OpenFlags]::ReadWrite)
    $store.Remove($cert)
    $store.Close()

    # Remove this cert from Trusted People too...
    $store = new-object
System.Security.Cryptography.X509Certificates.X509Store("TrustedPeople","LocalMachine")
    $store.Open([Security.Cryptography.X509Certificates.OpenFlags]::ReadWrite)
    $store.Remove($cert)
    $store.Close()
}

# Create the new cert
$name = new-object -com "X509Enrollment.CX500DistinguishedName.1"
$name.Encode("CN=" + $sqlServerName, 0)

$key = new-object -com "X509Enrollment.CX509PrivateKey.1"
$key.ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
$key.KeySpec = 1
$key.Length = 1024
$key.SecurityDescriptor = "D:PAI(A;;0xd01f01ff;;;SY)(A;;0xd01f01ff;;;BA)(A;;0x80120089;;;NS)"
$key.MachineContext = 1
$key.Create()

$serverauthoid = new-object -com "X509Enrollment.CObjectId.1"
$serverauthoid.InitializeFromValue("1.3.6.1.5.5.7.3.1")
$ekuoids = new-object -com "X509Enrollment.CObjectIds.1"
$ekuoids.add($serverauthoid)
$ekuext = new-object -com "X509Enrollment.CX509ExtensionEnhancedKeyUsage.1"
$ekuext.InitializeEncode($ekuoids)

$cert = new-object -com "X509Enrollment.CX509CertificateRequestCertificate.1"
$cert.InitializeFromPrivateKey(2, $key, "")
$cert.Subject = $name
$cert.Issuer = $cert.Subject
$cert.NotBefore = get-date
$cert.NotAfter = $cert.NotBefore.AddDays(3650)
$cert.X509Extensions.Add($ekuext)
$cert.Encode()

$enrollment = new-object -com "X509Enrollment.CX509Enrollment.1"
$enrollment.InitializeFromRequest($cert)
$enrollment.CertificateFriendlyName = "ConfigMgr SQL Server Identification Certificate"
$certdata = $enrollment.CreateRequest(0x1)
$enrollment.InstallResponse(0x2, $certdata, 0x1, "")

# Add this cert to the trusted peoples store
[Byte[]]$bytes = [System.Convert]::FromBase64String($certdata)

$trustedPeople = new-object System.Security.Cryptography.X509certificates.X509Store "TrustedPeople",
"LocalMachine"
$trustedPeople.Open([Security.Cryptography.X509Certificates.OpenFlags]::ReadWrite)
$trustedPeople.Add([Security.Cryptography.X509Certificates.X509Certificate2]$bytes)
$trustedPeople.Close()

# Get thumbprint from cert
$sha = new-object System.Security.Cryptography.SHA1CryptoServiceProvider
$certHash = $sha.ComputeHash($bytes)
$certHashCharArray = "";
$certThumbprint = "";
```

```
# Format the bytes into a hexadecimal string
foreach($byte in $certHash)
{
    $temp = ($byte | % {"{0:x}" -f $_}) -join ""
    $temp = ($temp | % {"{0,2}" -f $_})
    $certHashCharArray = $certHashCharArray+ $temp;
}
$certHashCharArray = $certHashCharArray.Replace(' ', '0');

# SQL needs the thumbprint in lower case
foreach($char in $certHashCharArray)
{
    [System.String]$myString = $char;
    $certThumbprint = $certThumbprint + $myString.ToLower();
}

# Configure SQL to use this cert
$path = "HKLM:\SOFTWARE\Microsoft\Microsoft SQL Server\Instance Names\SQL"
$subKey = (Get-ItemProperty $path).$sqlInstanceName
$realPath = "HKLM:\SOFTWARE\Microsoft\Microsoft SQL Server\" + $subKey +
"\MSSQLServer\SuperSocketNetLib"
$certKeyName = "Certificate"
Set-ItemProperty -path $realPath -name $certKeyName -Type string -Value $certThumbprint

# restart sql service
Restart-Service $SQLServiceName -Force
```

3. On the database replica server, run the following command that applies to the configuration of your SQL Server:

   - For a default instance of SQL Server: Right-click the file **CreateMPReplicaCert.ps1** and select **Run with PowerShell**. When the script runs, it creates the self-signed certificate and configures SQL Server to use the certificate.
   - For a named instance of SQL Server: Use PowerShell to run the command **%path%\CreateMPReplicaCert.ps1 xxxxxx** where **xxxxxx** is the name of the SQL Server instance.
   - After the script completes, verify that the SQL Server Agent is running. If not, restart the SQL Server Agent.

To configure remote management points to use the self-signed certificate of the database replica server

1. Perform the following steps on the database replica server to export the server's self-signed certificate:

   a. Click **Start**, click **Run**, and type **mmc.exe**. In the empty console, click **File**, and then click **Add/Remove Snap-in**.

   b. In the **Add or Remove Snap-ins** dialog box, select **Certificates** from the list of **Available snap-ins**, and then click **Add**.

   c. In the **Certificate snap-in** dialog box, select **Computer account**, and then click **Next**.

   d. In the **Select Computer** dialog box, ensure that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**.

   e. In the **Add or Remove Snap-ins** dialog box, click **OK**.

   f. In the console, expand **Certificates (Local Computer)**, expand **Personal**, and select **Certificates**.

   g. Right-click the certificate with the friendly name of **ConfigMgr SQL Server Identification Certificate**, click **All Tasks**, and then select **Export**.

h. Complete the **Certificate Export Wizard** by using the default options and save the certificate with the **.cer** file name extension.

2. Perform the following steps on the management point computer to add the self-signed certificate for the database replica server to the Trusted People certificate store on the management point:

   a. Repeat the preceding steps 1.a through 1.e to configure the **Certificate** snap-in MMC on the management point computer.

   b. In the console, expand **Certificates (Local Computer)**, expand **Trusted People**, right-click **Certificates**, select **All Tasks**, and then select **Import** to start the **Certificate Import Wizard**.

   c. On the **File to Import** page, select the certificate saved in step 1.h, and then click **Next**.

   d. On the **Certificate Store** page, select **Place all certificates in the following store**, with the **Certificate store** set to **Trusted People**, and then click **Next**.

   e. Click **Finish** to close the wizard and complete the certificate configuration on the management point.

Step 5 - Configure the SQL Server Service Broker for the database replica server

To support client notification with a database replica for a management point, you must configure communication between the site database server and the database replica server for the SQL Server Service Broker. This requires you to configure each database with information about the other database, and to exchange certificates between the two databases for secure communication.

> **NOTE**
> Before you can use the following procedure, the database replica server must successfully complete the initial synchronization with the site database server.

The following procedure does not modify the Service Broker port that is configured in SQL Server for the site database server or the database replica server. Instead, this procedure configures each database to communicate with the other database by using the correct Service Broker port.

Use the following procedure to configure the Service Broker for the site database server and the database replica server.

To configure the service broker for a database replica

1. Use **SQL Server Management Studio** to connect to database replica server database, and then run the following query to enable the Service Broker on the database replica server: **ALTER DATABASE <Replica Database Name> SET ENABLE_BROKER, HONOR_BROKER_PRIORITY ON WITH ROLLBACK IMMEDIATE**

2. Next, on the database replica server, configure the Service Broker for client notification and export the Service Broker certificate. To do this, run a SQL Server stored procedure that configures the Service Broker and exports the certificate as a single action. When you run the stored procedure, you must specify the FQDN of the database replica server, the name of the database replicas database, and specify a location for the export of the certificate file.

   Run the following query to configure the required details on the database replica server, and to export the certificate for the database replica server: **EXEC sp_BgbConfigSSBForReplicaDB '<Replica SQL Server FQDN>', '<Replica Database Name>', '<Certificate Backup File Path>'**

> **NOTE**
> When the database replica server is not on the default instance of SQL Server, for this step you must specify the instance name in addition to the replica database name. To do so, replace **<Replica Database Name>** with **<Instance name\Replica Database Name>**.

After you export the certificate from the database replica server, place a copy of the certificate on the primary sites database server.

3. Use **SQL Server Management Studio** to connect to the primary site database. After you connect to the primary sites database, run a query to import the certificate and specify the Service Broker port that is in use on the database replica server, the FQDN of the database replica server, and name of the database replicas database. This configures the primary sites database to use the Service Broker to communicate to the database of the database replica server.

   Run the following query to import the certificate from the database replica server and specify the required details: **EXEC sp_BgbConfigSSBForRemoteService 'REPLICA', '<SQL Service Broker Port>', '<Certificate File Path>', '<Replica SQL Server FQDN>', '<Replica Database Name>'**

   > **NOTE**
   > When the database replica server is not on the default instance of SQL Server, for this step you must specify the instance name in addition to the replica database name. To do so, replace **<Replica Database Name>** with **\Instance name\Replica Database Name>**.

4. Next, on the site database server, run the following command to export the certificate for the site database server: **EXEC sp_BgbCreateAndBackupSQLCert '<Certificate Backup File Path>'**

   After you export the certificate from the site database server, place a copy of the certificate on the database replica server.

5. Use **SQL Server Management Studio** to connect to the database replica server database. After you connect to the database replica server database, run a query to import the certificate and specify the site code of the primary site and the Service Broker port that is in use on the site database server. This configures the database replica server to use the Service Broker to communicate to the database of the primary site.

   Run the following query to import the certificate from the site database server: **EXEC sp_BgbConfigSSBForRemoteService '<Site Code>', '<SQL Service Broker Port>', '<Certificate File Path>'**

   A few minutes after you complete the configuration of the site database and the database replica database, the notification manager at the primary site sets up the Service Broker conversation for client notification from the primary site database to the database replica.

Supplemental script for additional database replicas on a single SQL Server

When you use the script from step 4 to configure a self-signed certificate for the database replica server on a SQL Server that already has a database replica you plan to continue using, you must use a modified version of the original script. The following modifications prevent the script from deleting an existing certificate on the server, and create subsequent certificates with unique Friendly names. Edit the original script as follows:

- Comment out (prevent from running) each line between the script entries **# Delete existing cert if one exists** and **# Create the new cert**. To do so, add a **#** as the first character of each applicable line.
- For each subsequent database replica you use this script to configure, update the Friendly name for the

certificate. To do so, edit the line **$enrollment.CertificateFriendlyName = "ConfigMgr SQL Server Identification Certificate"** and replace **ConfigMgr SQL Server Identification Certificate** with a new name, like **ConfigMgr SQL Server Identification Certificate1**.

Manage database replica configurations

When you use a database replica at a site, use the information in the following sections to supplement the process of uninstalling a database replica, uninstalling a site that uses a database replica, or moving the site database to a new installation of SQL Server. When you use information in the following sections to delete publications, use the guidance for deleting transactional replication for the version of SQL Server that you use for the database replica. For example, if you use SQL Server 2008 R2, see How to: Delete a Publication (Replication Transact-SQL Programming).

> **NOTE**
> After you restore a site database that was configured for database replicas, before you can use the database replicas you must reconfigure each database replica, recreating both the publications and subscriptions.

Uninstall a database replica

When you use a database replica for a management point, you might need to uninstall the database replica for a period of time, and then reconfigure it for use. For example, you must remove database replicas before you upgrade a Configuration Manager site to a new service pack. After the site upgrade completes, you can restore the database replica for use.

Use the following steps to uninstall a database replica.

1. In the **Administration** workspace of the Configuration Manager console, expand **Site Configuration**, then select **Servers and Site System Roles**, and then in the details pane select the site system server that hosts the management point that uses the database replica you will uninstall.
2. In the **Site System Roles** pane, right click **Management point** and select **Properties**.
3. On the **Management Point Database** tab, select **Use the site database** to configure the management point to use the site database instead of the database replica. Then, click **OK** to save the configuration.
4. Next, Use **SQL Server Management Studio** to perform the following tasks:
   - Delete the publication for the database replica from the site server database.
   - Delete the subscription for the database replica from the database replica server.
   - Delete the replica database from the database replica server.
   - Disable publishing and distribution on the site database server. To disable publishing and distribution, right-click the Replication folder and then click **Disable Publishing and Distribution**.
5. After you delete the publication, subscription, the replica database, and disable publishing on the site database server, the database replica is uninstalled.

Uninstall a site server that publishes a database replica

Before you uninstall a site that publishes a database replica, use the following steps to clean up the publication and any subscriptions.

1. Use **SQL Server Management Studio** to delete the database replica publication from the site server database.
2. Use **SQL Server Management Studio** to delete the database replica subscription from each remote SQL Server that hosts a database replica for this site.

3. Uninstall the site.

Move a site server database that publishes a database replica

When you move the site database to a new computer, use the following steps:

1. Use **SQL Server Management Studio** to delete the publication for the database replica from the site server database.
2. Use **SQL Server Management Studio** to delete the subscription for the database replica from each database replica server for this site.
3. Move the database to the new SQL Server computer. For more information, see the Modify the site database configuration section in the Modify your System Center Configuration Manager infrastructure topic.
4. Recreate the publication for the database replica on the site database server. For more information, see Step 1 - Configure the site database server to Publish the database replica in this topic.
5. Recreate the subscriptions for the database replica on each database replica server. For more information, see Step 2 - Configuring the database replica server in this topic.

Site components for Configuration Manager

5/9/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

For each Configuration Manager site, you can configure site components to modify the behavior of site system roles and site status reporting. Site component configurations apply to a site, and to each instance of an applicable site system role at the site.

In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. Select a site. In the **Settings** group of the ribbon, choose **Configure Site Components**. Select one of the following options:

- Software distribution
- Software update point
- Operating system deployment
- Management point
- Status reporting
- Email notification
- Collection membership evaluation

About site components

Most options for the various site components are self-explanatory when viewed in the Configuration Manager console. However, the following details can help explain some of the more complex configurations, or direct you to additional content.

> **NOTE**
> The available options for some components vary whether you select the central administration site, a primary site, or a secondary site. Some components are not available at all for certain types of sites.

Software distribution

Content distribution settings

On the **General** tab, specify settings that modify how the site server transfers content to its distribution points. When you increase the values you use for concurrent distribution settings, content distribution can use more network bandwidth.

Pull distribution point

For more information, see Use a pull-distribution point.

Network access account

For more information, see Network access account.

Software update point

For more information, see Install a software update point.

Operating system deployment

For more information, see Specify the drive for offline OS image servicing.

Management point

On the **General** tab, set up the site to publish information about its management points to Active Directory Domain Services.

Configuration Manager clients use management points to locate services, and to find site information such as boundary group membership and PKI certificate selection options. Clients also use management points to find other management points in the site, as well as distribution points from which to download software. Management points also help clients to complete site assignment, and to download client policy and upload client information.

The most secure method for clients to find management points is to publish them in Active Directory Domain Services. This service location method requires the following to be true:

- The schema is extended for Configuration Manager.
- There's a **System Management** container, with appropriate security permissions for the site server to publish to this container.
- The Configuration Manager site is set up to publish to Active Directory Domain Services.
- Clients belong to the same Active Directory forest as the site server's forest.

When clients on the intranet can't use Active Directory Domain Services to find management points, use DNS publishing.

For general information about service location, see Understand how clients find site resources and services.

Publish selected intranet management points in DNS

Specify this option when clients on the intranet can't find management points from Active Directory Domain Services. Instead, they can use a DNS service location resource record (SRV RR) to find a management point in their assigned site.

For Configuration Manager to publish intranet management points to DNS, all the following conditions must be met:

- Your DNS servers have a version of BIND that is 8.1.2 or later.
- Your DNS servers are set up for automatic updates, and support service location resource records.
- The specified fully qualified domain names (FQDNs) for the management points in Configuration Manager have host entries (A or AAA records) in DNS.

> **WARNING**
> For clients to find management points that are published in DNS, you must assign the clients to a specific site (rather than use automatic-site assignment). Set up these clients to use the site code with the domain suffix of their management point. For more information, see Locating management points.

If Configuration Manager clients can't use Active Directory Domain Services or DNS to find management points on the intranet, they use WINS. The first management point that is installed for the site is automatically published to WINS when it's set up to accept HTTP client connections on the intranet.

Status reporting

These settings directly set up the level of detail that's included in status reports from sites and clients.

Email notification

Specify account and email server details to enable Configuration Manager to send email notifications for alerts.

For more information, see Use alerts and the status system.

Collection membership evaluation

Use this component to set how often collection membership is incrementally evaluated. Incremental evaluation

updates a collection membership with only new or changed resources.

For more information, see Best practices for collections.

Use the Configuration Manager Service Manager to manage site components

You can use the Configuration Manager Service Manager to control Configuration Manager services, and to view the status of any Configuration Manager service or working thread. These services and threads are referred to collectively as Configuration Manager components. Understand the following statements about Configuration Manager components:

- Components can run on any site system.
- Components are managed the same way that you manage services in Windows. You can start, stop, pause, resume, or query Configuration Manager components.

A Configuration Manager service runs when there's something for it to do. This action is typically when a configuration file is written to a component's inbox.

Use the Configuration Manager Service Manager

1. In the Configuration Manager console, go to the **Monitoring** workspace, expand **System Status**, and select the **Component Status** node.
2. In the **Component** group of the ribbon, select **Start**, and then choose **Configuration Manager Service Manager**.
3. When the Configuration Manager Service Manager opens, connect to the site that you want to manage.

   If you don't see the site that you want to manage, go to the **Site** menu, and select **Connect**. Then enter the name of the site server of the correct site.
4. Expand the site and navigate to **Components** or **Servers**, depending on where the components that you want to manage are located.
5. In the right pane, select one or more components. Then on the **Component** menu, select **Query** to update the status of your selection.
6. After the status of the component is updated, use one of the four action-based options on the **Component** menu to modify the component's operation. After you request an action, you must query the component to display the new status of the component.
7. Close the Configuration Manager Service Manager when you're finished modifying the operational status of components.

Publish site data for System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

After you extend the Active Directory schema for System Center Configuration Manager, you can publish Configuration Manager sites to Active Directory Domain Services (AD DS). This lets Active Directory computers securely retrieve site information from a trusted source. Although publishing site information to AD DS is not required for basic Configuration Manager functionality, it can reduce administrative overhead to do so.

- **When a site is configured to publish to AD DS**, Configuration Manager clients can automatically find management points through Active Directory publishing. They use an LDAP query to a global catalog server.
- **When a site does not publish to AD DS**, clients must have an alternative mechanism to locate their default management point.

For information about how clients find a management point, see Understand how clients find site resources and services for System Center Configuration Manager.

Configure sites to publish to AD DS

The following are the high-level steps:

- You must extend the Active Directory schema for System Center Configuration Manager in each forest where you will publish site data. Also ensure the **System Management** container is present.
- You must grant the computer account of each primary site that will publish data **full control** to the **System Management** container, and all of its child objects.

To enable a Configuration Manager site to publish site information to Active Directory forest

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Site Configuration**, and click **Sites**. Select the site that you want to have publish its site data. Then on the **Home** tab, in the **Properties** group, click **Properties**.
3. On the **Publishing** tab of the site's properties, select the forests to which this site will publish site data.
4. Click **OK** to save the configuration.

To set up Active Directory forests for publishing

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Hierarchy Configuration**, and click **Active Directory Forests**. If Active Directory Forest Discovery has previously run, you see each discovered forest in the results pane. The local forest and any trusted forests are discovered when Active Directory Forest Discovery runs. Only untrusted forests must be manually added.
   - To set up a previously discovered forest, select the forest in the results pane. Then on the **Home** tab, in the **Properties** group, click **Properties** to open the forest properties. Continue with step 3.
   - To set up a new forest that is not listed, on the **Home** tab, in the **Create** group, click **Add Forest** to

open the **Add Forests** dialog box. Continue with step 3.

3. On the **General** tab, complete configurations for the forest that you want to discover, and specify the **Active Directory Forest Account**.

   > **NOTE**
   > Active Directory Forest Discovery requires a global account to discover and publish to untrusted forests. If you do not use the computer account of the site server, you can only select a global account.

4. If you plan to allow sites to publish site data to this forest, on the **Publishing** tab, complete configurations for publishing to this forest.

   > **NOTE**
   > If you enable sites to publish to a forest, you must extend the Active Directory schema of that forest for Configuration Manager. The Active Directory Forest Account must have Full Control permissions to the System container in that forest.

5. When you complete the configuration of this forest for use with Active Directory Forest Discovery, click **OK** to save the configuration.

Manage content and content infrastructure for System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

When you are ready to set up and then manage your content management infrastructure for System Center Configuration Manager, use the information in the following topics:

- Install and configure distribution points for System Center Configuration Manager. Before you can deploy content, you must install and set up distribution points. Then you can set up distribution point groups to help simplify management of content across your infrastructure. The information in this topic can help you complete these tasks, and details the deep and varied settings supported by individual distribution points.
- Deploy and manage content for System Center Configuration Manager. Content deployment transfers files and software to distribution point servers throughout your network. In addition to a simple transfer, you can prestage content, which is a method that can help you avoid excessive use of network bandwidth. The information in this topic can help you with the basic tasks of sending that content or using pre-staged content effectively.
- Monitor content you have distributed with System Center Configuration Manager. As you deploy content, you can monitor its status across your infrastructure. You can also redistribute content that fails to reach distribution points, or cancel distributions that remain in progress. The information in this topic helps you understand how to monitor your content, including how to fix some problems when the transfer of content fails.

Install and configure distribution points in Configuration Manager

7/26/2019 • 27 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Install Configuration Manager distribution points to host the content files that you deploy to devices and users. Create distribution point groups to simplify how you manage distribution points, and how you distribute content to distribution points.

You *install a new distribution point* by using the installation wizard. For more information, see Install a distribution point. To *manage the properties of an existing distribution point*, edit the properties of the distribution point. For more information, see Configure a distribution point.

Configure most of the distribution point settings with either method. A few settings are available only when you're either installing or editing, but not both:

- Settings that are available only when you're installing a distribution point:
  - **Allow Configuration Manager to install IIS on the distribution point computer**
  - **Configure drive space settings for the distribution point**
- Settings that are available only when you're editing the properties of a distribution point:
  - **Manage distribution point group relationships**
  - **View Content deployed to the distribution point**
  - **Configure Rate limits for data transfers to distribution points**
  - **Configure Schedules for data transfers to distribution points**

Install a distribution point

Choose a site system server as a distribution point before content can be made available to client computers. Assign a distribution point to at least one boundary group before on-premises client computers can use that distribution point as a content source location. Add the distribution point role to a new site system server, or add it to an existing site system server.

Prerequisites

When you install a new distribution point, you use an installation wizard that walks you through the available settings. Before you start, consider the following prerequisites:

- You must have the following security permissions to create and configure a distribution point:
  - **Read** for the **Distribution Point** object
  - **Copy to Distribution Point** for the **Distribution Point** object
  - **Modify** for the **Site** object
  - **Manage Certificates for Operating System Deployment** for the **Site** object
- Install Internet Information Services (IIS) on the Windows server that hosts the distribution point. Or, when you install the site system role, Configuration Manager can install and configure IIS for you.

Procedure to install a distribution point

Use this procedure to add a new distribution point. To change the configuration of an existing distribution point, see the Configure a distribution point section.

Start with the general procedure to Install site system roles. Select the **Distribution point** role on the **System Role Selection** page of the Create Site System Server wizard. This action adds the following pages to the wizard:

- Distribution point
- Communication
- Drive Settings
- Pull Distribution Point
- PXE Settings
- Multicast
- Content Validation
- Boundary Groups

> **IMPORTANT**
> The following settings are available only when you're installing a distribution point:
>
> - **Allow Configuration Manager to install IIS on the distribution point computer**
> - **Configure drive space settings for the distribution point**

For more information on the pages of the wizard specific to the distribution point role, see the Configure a distribution point section. For example, if you want to install the distribution point as a pull-distribution point, choose the option to **Enable this distribution point to pull content from other distribution points**. Then make the additional configurations that pull-distribution points require.

After you finish the Create Site System Server wizard, the site adds the distribution point role to the site system server.

Manage distribution point groups

Distribution point groups provide a logical grouping of distribution points for content distribution. Use these groups to manage and monitor content from a central location for distribution points that span multiple sites. Keep the following point in mind:

- Add one or more distribution points from any site in the hierarchy to a distribution point group.
- Add a distribution point to more than one distribution point group.
- When you distribute content to a distribution point group, Configuration Manager distributes the content to all distribution points that are members of the group.
- If you add a distribution point to the group after an initial content distribution, Configuration Manager automatically distributes the content to the new distribution point member.
- Associate a collection with a distribution point group. When you distribute content to that collection, Configuration Manager determines which groups are associated with the collection. It then distributes the content to all distribution points that are members of those groups.

> **NOTE**
> After you distribute content to a collection, if you then associate the collection with a new distribution point group, you must redistribute the content to the collection before the content is distributed to the new distribution point group.

The next sections list the procedures for the following actions to manage distribution point groups:

- Create and configure a new distribution point group
- Modify an existing distribution point group
- Add selected distribution points to existing distribution point groups

Procedure to create and configure a new distribution point group

1. In the Configuration Manager console, go to the **Administration** workspace, and select the **Distribution Point Groups** node.
2. In the ribbon, select **Create Group**.
3. In the Create New Distribution Point Group window, enter the **Name**, and optionally a **Description** for the group.
4. On the **Members** tab, select **Add**.
5. In the Add Distribution Points window, select one or more distribution points to add as members of the group. Then choose **OK**.
6. If necessary, switch to the **Collections** tab of the Create New Distribution Point Group window, and select **Add**.
7. In the Select Collections window, select the collections to associate with the distribution point group, and then choose **OK**.
8. In the Create New Distribution Point Group window, choose **OK** to create the group.

Create a new group from an existing distribution point

1. In the Configuration Manager console, go to the **Administration** workspace, and select the **Distribution Points** node. Select one or more distribution points to add to a new distribution point group.
2. In the ribbon, select **Add Selected Items**, and then select **Add Selected Items to New Distribution Point Group**.

This process automatically populates the **Members** tab of the Create New Distribution Point Group window with the selected servers.

Procedure to modify an existing distribution point group

1. In the Configuration Manager console, go to the **Administration** workspace, and select the **Distribution Point Groups** node.
2. Select an existing distribution point group to modify. In the ribbon, select **Properties**.
3. To associate new collections with this group, switch to the **Collections** tab, and choose **Add**. Select the collections, and then choose **OK**.
4. To add new distribution points to this group, switch to the **Members** tab, and choose **Add**. Select the distribution points, and then choose **OK**.
5. Choose **OK** to save changes to the distribution point group.

Procedure to add selected distribution points to existing distribution point groups

1. In the Configuration Manager console, go to the **Administration** workspace, and select the **Distribution Points** node. Select one or more distribution points to add to an existing group.
2. In the ribbon, select **Add Selected Items**, and then select **Add Selected Items to Existing Distribution Point Groups**.
3. In the **Available distribution point groups**, select the groups to which the selected distribution points are added as members. Then choose **OK**.

Reassign a distribution point

Many customers have large Configuration Manager infrastructures, and are reducing primary or secondary sites to simplify their environment. They still need to retain distribution points at branch office locations to serve content to managed clients. These distribution points often contain multiple terabytes or more of content. This content is costly in terms of time and network bandwidth to distribute to these remote servers.

This feature lets you reassign a distribution point to another primary site without redistributing the content. This action updates the site system assignment while persisting all of the content on the server. If you need to reassign multiple distribution points, first perform this action on a single distribution point. Then proceed with additional servers one at a time.

> **IMPORTANT**
> The target server can only host the distribution point role. If the site system server hosts another Configuration Manager server role, such as the state migration point, you cannot reassign the distribution point. You cannot reassign a cloud distribution point.

Before reassigning a distribution point, add the computer account of the destination site server to the local Administrator group on the target distribution point server.

Follow these steps to reassign a distribution point:

1. In the Configuration Manager console, connect to the central administration site.
2. Go to the **Administration** workspace, and select the **Distribution Points** node.
3. Right-click the target distribution point, and select **Reassign Distribution Point**.
4. Select the target site server and site code to which you want to reassign this distribution point.

Monitor the reassignment similarly as when you add a new role. The simplest method is to refresh the console view after several minutes. Add the site code column to the view. This value changes when Configuration Manager reassigns the server. If you try to perform another action on the target server before you refresh the console view, an "object not found" error occurs. Ensure the process is complete and refresh the console view before starting any other actions on the server.

After reassigning a distribution point, refresh the server's certificate. The new site server needs to re-encrypt this certificate using its public key and store it in the site database. For more information, see the **Create a self-signed certificate or import a public key infrastructure (PKI) client certificate for the distribution point** setting on the General tab of the distribution point properties.

- For PKI certificates, you don't need to create a new certificate. Import the same .PFX and enter the password.
- For self-signed certificates, adjust the expiration date or time to update it.
- If you don't refresh the certificate, the distribution point still serves content, but the following functions fail:

- Content validation messages (the distmgr.log shows that it can't decrypt the certificate)
- PXE support for clients

Tips

- Perform this action from the central administration site. This practice helps with replication to the primary sites.
- Don't distribute content to the target server and then attempt to reassign it. Distribute content tasks that are in progress may fail during the reassignment process, but it retries per normal.
- If the server is also a Configuration Manager client, make sure to also reassign the client to the new primary site. This step is especially critical for pull-distribution points, which use client components to download content.
- This process removes the distribution point from the old site's default boundary group. You need to manually add it to the new site's default boundary group, if necessary. All other boundary group assignments remain the same.

Maintenance mode

Starting in version 1902, you can set a distribution point in maintenance mode. Enable maintenance mode when you're installing software updates, or making hardware changes to the server.

While the distribution point is in maintenance mode, it has the following behaviors:

- The site doesn't distribute any content to it.
- Management points don't return the location of this distribution point to clients.
- When you update the site, a distribution point in maintenance mode still updates.
- The distribution point properties are read-only. For example, you can't change the certificate or add boundary groups.
- Any scheduled task, like content validation, still runs on the same schedule.

Be careful about enabling maintenance mode on more than one distribution point. This action may cause a performance impact to your other distribution points. Depending upon your boundary group configurations, clients may have increased download times or be unable to download content.

Enable maintenance mode

To put a distribution point in maintenance mode, your user account requires the **Modify** permission on the **Site** class. For example, the **Infrastructure Administrator** and **Full Administrator** built-in roles have this permission.

1. In the Configuration Manager console, go to the **Administration** workspace.
2. Select the **Distribution Points** node.
3. Select the target distribution point, and choose **Enable maintenance mode** from the ribbon.

To view the current state of the distribution points, add the "Maintenance mode" column to the **Distribution Points** node in the console.

For more information on automating this process with the Configuration Manager SDK, see SetDPMaintenanceMode method in class SMS_DistributionPointInfo.

Configure a distribution point

Individual distribution points support a variety of different configurations. However, not all distribution point types

support all configurations. For example, cloud distribution points don't support PXE- or multicast-enabled deployments. For more information about specific limitations, see the following articles:

- Use a cloud distribution point
- Use a pull-distribution point

The following sections describe the distribution point configurations when you're installing a new one or editing an existing one:

- General settings
- Communication
- Drive Settings
- Firewall Settings
- Pull Distribution Point
- PXE Settings
- Multicast
- Content Validation
- Boundary Groups

Procedure to change a distribution point

1. In the Configuration Manager console, go to the **Administration** workspace, and select the **Distribution Points** node.
2. Select the distribution point to configure. In the ribbon, choose **Properties**.
3. Use the information in the following sections when you're editing the properties of the distribution point.
4. After you make the changes that you want, select **OK** to save your settings and close the distribution point properties.

General

> **NOTE**
> In version 1902 and earlier, this page has additional settings for HTTP/HTTPS and certificates. Starting in version 1906, these settings are now on the Communication page.

The following settings are on the **Distribution point** page of the Create Site System Server wizard, and the **General** tab of the distribution point properties window:

- **Description**: An optional description for this distribution point role.
- **Install and configure IIS if required by Configuration Manager**: If IIS isn't already installed on the server, Configuration Manager installs and configures it. Configuration Manager requires IIS on all distribution points. If you don't choose this setting, and IIS isn't installed on the server, first install IIS before Configuration Manager can successfully install the distribution point.

  > **NOTE**
  > This option is only on the **Distribution point** page of the Create Site System Server wizard. It's available only when you're installing a new distribution point.

- **Enable and configure BranchCache for this distribution point**: Choose this setting to let Configuration Manager configure Windows BranchCache on the distribution point server. For more information, see BranchCache.

- **Adjust the download speed to use the unused network bandwidth (Windows LEDBAT)**: Starting in version 1806, enable distribution points to use network congestion control. For more information, see Windows LEDBAT. Minimum requirements for LEDBAT support:
  - Configuration Manager version 1806 (general release)
    - Windows Server, version 1709 or later
  - Configuration Manager version 1806 with update rollup (4462978), or later
    - Windows Server, version 1709 or later
    - Windows Server 2016 with updates KB4132216 and KB4284833
  - Configuration Manager version 1810 or later:
    - Windows Server, version 1709 or later
    - Windows Server 2016 with updates KB4132216 and KB4284833
    - Windows Server 2019
- **Enable this distribution point for prestaged content**: This setting enables you to add content to the server before you distribute software. Because the content files are already in the content library, they don't transfer over the network when you distribute the software. For more information, see Prestaged content.
- **Enable this distribution point to be used as Delivery Optimization In-Network Cache server**: Starting in version 1906, you can install a Delivery Optimization In-Network Cache (DOINC) server on your distribution points. By caching this content on-premises, your clients can benefit from the Delivery Optimization feature, but you can help to protect WAN links. For more information, including description of the additional settings, see Delivery Optimization In-Network Cache in Configuration Manager.

Communication

> **NOTE**
> Starting in version 1906, the following settings are on the **Communication** tab. In version 1902 and earlier, these settings are on the General tab.

The following settings are on the **Communication** page of the Create Site System Server wizard and the distribution point properties window:

- **Configure how client devices communicate with the distribution point**: There are advantages and disadvantages to using **HTTP** or **HTTPS**. For more information, see Security best practices for content management.
- **Allow clients to connect anonymously**: This setting specifies whether the distribution point allows anonymous connections from Configuration Manager clients to the content library.

  > **IMPORTANT**
  > If you don't use this setting, apply the changes described in Microsoft Knowledge Base article 2619572 on Windows 7 clients. Otherwise repair of Windows Installer applications can fail.
  >
  > When you deploy a Windows Installer application, the Configuration Manager client downloads the file to its local cache. The client eventually removes the files after the installation finishes. The Configuration Manager client updates the Windows Installer source list for the application. It sets the content path to the content library on associated distribution points. Later, if you try to repair the application on the device, MSIExec attempts to access the content path by using an anonymous user.
  >
  > After you install the update on clients and modify the documented registry key, MSIExec accesses the content path by using the signed-in user account.

- **Create a self-signed certificate or import a PKI client certificate**: Configuration Manager uses this certificate for the following purposes:

  - It authenticates the distribution point to a management point before the distribution point sends status messages.
  - When you **Enable PXE support for clients** on the **PXE Settings** page, the distribution point sends it to computers that PXE boot. These computers then use it to connect to a management point during the OS deployment process.

  When you configure all your management points in the site for HTTP, select the option to **Create self-signed certificate**. When you configure the management points for HTTPS, use the option to **Import certificate** from PKI.

  To import the certificate, browse to a valid Public Key Cryptography Standard (PKCS #12) file. This PFX or CER file has the PKI certificate with the following requirements for Configuration Manager:

  - The intended use includes client authentication
  - Enable the private key to be exported

  > **TIP**
  > There are no specific requirements for the certificate subject or subject alternative name (SAN). If necessary, use the same certificate for multiple distribution points.

  For more information about the certificate requirements, see PKI certificate requirements.

  For an example deployment of this certificate, see Deploying the client certificate for distribution points.

Drive settings

> **NOTE**
> These options are available only when you're installing a new distribution point.

Specify the drive settings for the distribution point. Configure up to two disk drives for the content library and two disk drives for the package share. Configuration Manager can use additional drives when the first two reach the configured drive space reserve. The **Drive Settings** page configures the priority for the disk drives and the amount of free disk space that remains on each disk drive.

- **Drive space reserve (MB)**: This value determines the amount of free space on a drive before Configuration Manager chooses a different drive and continues the copy process to that drive. Content files can span multiple drives.
- **Content locations**: Specify the locations for the content library and package share on this distribution point. By default, all content locations are set to **Automatic**. Configuration Manager copies content to the primary content location until the amount of free space reaches the value specified for **Drive space reserve (MB)**. When you select **Automatic**, Configuration Manager sets the primary content locations to the disk drive with the most disk space at installation. It sets the secondary locations to the disk drive with the second-most free disk space. When the primary and secondary locations reach the drive space reserve, Configuration Manager selects another available drive with the most free disk space to continue the copy process.

> **TIP**
> To prevent Configuration Manager from installing on a specific drive, create an empty file named **no_sms_on_drive.sms** and copy it to the root folder of the drive before you install the distribution point.

For more information, see The content library.

Firewall Settings

The distribution point must have the following inbound rules configured in the Windows firewall:

- Windows Management Instrumentation (DCOM-In)
- Windows Management Instrumentation (WMI-In)

Without these rules clients will receive error 0x801901F4 in DataTransferService.log when attempting to download content.

Pull distribution point

When you **Enable this distribution point to pull content from other distribution points**, it becomes a pull-distribution point. You change the behavior of how the distribution point gets the content that you distribute to it. For more information, see Use a pull-distribution point.

For each pull-distribution point that you configure, specify one or more source distribution points from which it gets the content:

- Choose **Add**, and then select one or more of the available distribution points to be sources.
- Use the arrow buttons to adjust the priority. When the pull-distribution point attempts to transfer content, the priority is the order in which it contacts the source distribution points. It first contacts distribution points with the lowest value.

PXE

Specify whether to enable PXE on the distribution point. Use PXE to start OS deployments on clients. For more information on how to use PXE in Configuration Manager, see Use PXE to deploy Windows over the network.

When you enable PXE, Configuration Manager installs Windows Deployment Services (WDS) on the server, if necessary. WDS is the service that performs the PXE boot to install operating systems. After you finish the wizard to create the distribution point, Configuration Manager installs a provider in WDS that uses the PXE boot functions.

Starting in version 1806, you can enable PXE on a distribution point without WDS.

Select the option to **Enable PXE support for clients**, and then configure the following settings:

> **NOTE**
> Select **Yes** in the **Review Required Ports for PXE** dialog box to confirm that you want to enable PXE. Configuration Manager automatically configures the default ports on Windows firewall. If you use a different firewall, manually configure the ports.
>
> If you install WDS and DHCP on the same server, configure WDS to listen on a different port. By default, DHCP listens on the same port. For more information, see Considerations when you have WDS and DHCP on the same server.

- **Allow this distribution point to respond to incoming PXE requests**: Specify whether to enable WDS to respond to PXE service requests. Use this setting to enable and disable the service without removing the PXE functionality from the distribution point.
- **Enable unknown computer support**: Specify whether to enable support for computers that

Configuration Manager doesn't manage. For more information, see Prepare for unknown computer deployments.

- **Enable a PXE responder without Windows Deployment Service**: Starting in version 1806, this option enables a PXE responder on the distribution point, which doesn't require WDS. This PXE responder supports IPv6 networks. If you enable this option on a distribution point that's already PXE-enabled, Configuration Manager suspends the WDS service. If you disable this option, but still **Enable PXE support for clients**, then the distribution point enables WDS again.

  > **NOTE**
  >
  > In version 1810 and earlier, it's not supported to use the PXE responder without WDS on servers that are also running a DHCP server.
  >
  > Starting in version 1902, when you enable a PXE responder on a distribution point without Windows Deployment Service, it can now be on the same server as the DHCP service.

- **Require a password when computers use PXE**: To provide additional security for your PXE deployments, specify a strong password.

- **User device affinity**: Specify how you want the distribution point to associate users with the destination computer for PXE deployments. Choose one of the following options:

  - **Allow user device affinity with auto-approval**: Choose this setting to automatically associate users with the destination computer without waiting for approval.
  - **Allow user device affinity pending administrator approval**: Choose this setting to wait for approval from an administrative user before users are associated with the destination computer.
  - **Do not allow user device affinity**: Choose this setting to specify that users aren't associated with the destination computer. This setting is the default.

    For more information about user device affinity, see Link users and devices with user device affinity.

- **Network interfaces**: Specify that the distribution point responds to PXE requests from all network interfaces or from specific network interfaces. If the distribution point responds to specific network interfaces, then provide the MAC address for each network interface.

  > **NOTE**
  >
  > When changing the network interface, restart the WDS service to make sure it properly saves the configuration. Starting in version 1806, when using the PXE responder service, restart the **ConfigMgr PXE Responder Service** (SccmPxe).

- **Specify the PXE server response delay (seconds)**: When you use multiple PXE servers, specify how long this PXE-enabled distribution point should wait before it responds to computer requests. By default, the Configuration Manager PXE-enabled distribution point responds immediately.

Multicast

Specify whether to enable multicast on the distribution point. Multicast deployments conserve network bandwidth by simultaneously sending data to multiple Configuration Manager clients. Without multicast, the server sends a copy of the data to each client over a separate connection. For more information about using multicast for OS deployment, see Use multicast to deploy Windows over the network.

When you enable multicast, Configuration Manager installs Windows Deployment Services (WDS) on the server, if necessary.

Select the option to **Enable multicast to simultaneously send data to multiple clients**, and then configure the following settings:

- **Multicast Connection Account**: Specify the account to use when you configure Configuration Manager database connections for multicast. For more information, see the Multicast connection account.
- **Multicast address settings**: Specify the IP addresses for sending data to the destination computers. By default, it obtains the IP address from a DHCP server that's enabled to distribute multicast addresses. Depending on the network environment, you can specify a range of IP addresses from 239.0.0.0 through 239.255.255.255.

  > **IMPORTANT**
  > The IP addresses that you configure must be accessible by the destination computers that request the OS image. Verify that routers and firewalls allow for multicast traffic between the destination computer and the distribution point.

- **UDP port range for multicast**: Specify the range of UDP ports that are used to send data to the destination computers.

  > **IMPORTANT**
  > The UDP ports must be accessible by the destination computers that request the OS image. Verify that routers and firewalls allow for multicast traffic between the destination computer and the site server.

- **Maximum clients**: Specify the maximum number of destination computers that can download the OS image from this distribution point.
- **Enable scheduled multicast**: Specify how Configuration Manager controls when to start deploying operating systems to destination computers. Configure the following options:
  - **Session start delay (minutes)**: Specify the number of minutes that Configuration Manager waits before it responds to the first deployment request.
  - **Minimum session size (clients)**: Specify how many requests must be received before Configuration Manager starts to deploy the operating system.

> **IMPORTANT**
> Starting in version 1806, to enable and configure multicast on the **Multicast** tab of the distribution point properties, the distribution point must use Windows Deployment Service.
>
> - If you **Enable PXE support for clients** and **Enable multicast to simultaneously send data to multiple clients**, then you can't **Enable a PXE responder without Windows Deployment Service**.
> - If you **Enable PXE support for clients** and **Enable a PXE responder without Windows Deployment Service**, then you can't **Enable multicast to simultaneously send data to multiple clients**

Group relationships

> **NOTE**
> These options are available only when you're editing the properties of a previously installed distribution point.

Manage the distribution point groups in which this distribution point is a member.

To add this distribution point as a member to an existing a distribution point group, choose **Add**. In the Add to Distribution Point Groups window, select an existing group, and then choose **OK**.

To remove this distribution point from a distribution point group, select the group in the list, and then choose **Remove**. Removing the distribution point from a distribution point group does not remove any content from the distribution point.

Content

> **NOTE**
> These options are available only when you're editing the properties of a previously installed distribution point.

Manage the content that you distributed to the distribution point. Select from the list of deployment packages, and perform the following actions:

- **Validate**: Start the process to validate the integrity of the content files for the software. To view the results of the content validation process, in the **Monitoring** workspace, expand **Distribution Status**, and then choose the **Content Status** node. For more information, see Validate content.
- **Redistribute**: Copies all of the content files for the selected software to the distribution point, and overwrites the existing files. You typically use this action to repair content files. For more information, see Redistribute content.
- **Remove**: Removes the content files for the software from the distribution point. For more information, see Remove content.

Content validation

Set a schedule to validate the integrity of content files on the distribution point. When you enable content validation on a schedule, Configuration Manager starts the process at the scheduled time. It verifies all content on the distribution point based on the local SMS_PackagesInContLib SCCMDP class. You can also configure the content validation priority. By default, the priority is set to **Lowest**. Increasing the priority might increase the processor and disk utilization on the server during the validation process, but it should complete faster.

To view the results of the content validation process, in the **Monitoring** workspace, expand **Distribution Status**, and then choose the **Content Status** node. It shows the content for each software type, for example, application, software update package, and boot image.

> **WARNING**
> Although you specify the content validation schedule by using the local time for the computer, the Configuration Manager console shows the schedule in UTC.

For more information, see Validate content.

Boundary groups

Manage the boundary groups to which you assign this distribution point. Add the distribution point to at least one boundary group. During content deployment, clients must be in a boundary group associated with a distribution point to use that distribution point as a source location for content.

Configure boundary group *relationships* that define when and to which boundary groups a client can fall back to find content. For more information, see Boundary groups.

Choose **Add** and select an existing boundary group from the list.

To create a new boundary group for this distribution point, choose **Create**. For more information on how to create

and configure a boundary group, see Procedures for boundary groups.

When you're editing the properties of a previously installed distribution point, manage the option to **Enable for on-demand distribution**. This option allows Configuration Manager to automatically distribute content to this server when a client requests it. For more information, see On-demand content distribution.

Schedule

> **NOTE**
> These options are available only when you're editing the properties of a previously installed distribution point.
>
> This tab is available only when you edit the properties for a distribution point that's remote from the site server.

Configure a schedule that restricts when Configuration Manager can transfer data to the distribution point. Restrict data by priority or close the connection for selected time periods.

To restrict data, select the time period in the grid, and then choose one of the following settings for **Availability**:

- **Open for all priorities**: Configuration Manager sends data to the distribution point with no restrictions. This setting is the default for all time periods.
- **Allow medium and high priority**: Configuration Manager sends only medium-priority and high-priority data to the distribution point.
- **Allow high priority only**: Configuration Manager sends only high-priority data to the distribution point.
- **Closed**: Configuration Manager doesn't send any data to the distribution point.

Configure the **Distribution priority** of software on the **Distribution Settings** tab of the software's properties.

> **IMPORTANT**
> The schedule is based on the time zone from the sending site, not the distribution point.

Rate limits

> **NOTE**
> These options are available only when you're editing the properties of a previously installed distribution point.
>
> This tab is available only when you edit the properties for a distribution point that's remote from the site server.

Configure rate limits to control the network bandwidth that Configuration Manager uses to transfer content to the distribution point. Choose from the following options:

- **Unlimited when sending to this destination**: Configuration Manager sends content to the distribution point with no rate limit restrictions. This setting is the default.
- **Pulse mode**: This option specifies the size of the data blocks that the site server sends to the distribution point. You can also specify a time delay between sending each data block. Use this option when you must send data across a very low-bandwidth network connection to the distribution point. For example, you have constraints to send 1 KB of data every five seconds, regardless of the speed of the link or its usage at a given time.
- **Limited to specified maximum transfer rates by hour**: Specify this setting to have a site send data to a distribution point by using only the percentage of time that you configure. When you use this option, Configuration Manager doesn't identify the network's available bandwidth. Instead it divides the time that it

can send data. The server sends data for a short period of time, which is followed by periods of time when data isn't sent. For example, if you set **Limit available bandwidth** to **50%**, Configuration Manager transmits data for a period of time followed by an equal period of time when no data is sent. The actual size amount of data, or size of the data block, isn't managed. It only manages the amount of time during which it sends data.

Deploy and manage content for System Center Configuration Manager

7/19/2019 • 25 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

After you install distribution points for System Center Configuration Manager, you can begin to deploy content to them. Typically, content transfers to distribution points across the network, but other options to get content to the distribution points exists. After content transfers to a distribution point, you can update, redistribute, remove, and validate that content on distribution points.

Distribute content

Typically, you distribute content to distribution points so that it is available to client computers. (The exception to this is when you use on-demand content distribution for a specific deployment.) When you distribute content, Configuration Manager stores content files in a package, and then distributes the package to the distribution point. Types of content that you can distribute, include:

- Application deployment types
- Packages
- Deployment packages
- Driver packages
- Operating system images
- Operating system installers
- Boot images
- Task sequences

When you create a package that contains source files, such as an application deployment type or deployment package, the site on which the package is created becomes the site owner for the package content source. Configuration Manager copies the source files from the source file path that you specify for the object to the content library on the site server that owns the package content source. Then, Configuration Manager replicates the information to additional sites. (See The content library for more information about this.)

Use the following procedure to distribute content to distribution points.

To distribute content on distribution points

1. In the Configuration Manager console, click **Software Library**.
2. In the **Software Library** workspace, select one of the following steps for the type of content that you want to distribute:
   - **Applications**: Expand **Application Management** > **Applications**, and then select the applications that you want to distribute.
   - **Packages**: Expand **Application Management** > **Packages**, and then select the packages that you want to distribute.
   - **Deployment Packages**: Expand **Software Updates** > **Deployment Packages**, and then select the

deployment packages that you want to distribute.

- **Driver Packages**: Expand **Operating Systems** > **Driver Packages**, and then select the driver packages that you want to distribute.
- **Operating System Images**: Expand **Operating Systems** > **Operating System Images**, and then select the operating system images that you want to distribute.
- **Operating System Installers**: Expand **Operating Systems** > **Operating System Installers**, and then select the operating system installers that you want to distribute.
- **Boot Images**: Expand **Operating Systems** > **Boot Images**, and then select the boot images that you want to distribute.
- **Task Sequences**: Expand **Operating Systems** > **Task Sequences**, and then select the task sequence that you want to distribute. Although task sequences do not contain content, they have associated content dependencies that are distributed.

  > **NOTE**
  > If you modify the task sequence, you must redistribute the content.

3. On the **Home** tab, in the **Deployment** group, click **Distribute Content**. The Distribute Content Wizard opens.
4. On the **General** page, verify that the content listed is the content that you want to distribute, choose whether you want Configuration Manager to detect content dependencies that are associated with the selected content and add the dependencies to the distribution, and then click **Next**.

   > **NOTE**
   > You have the option to configure the **Detect associated content dependencies and add them to this distribution** setting only for the application content type. Configuration Manager automatically configures this setting for task sequences, and it cannot be modified.

5. On the **Content** tab, if displayed, verify that the content listed is the content that you want to distribute, and then click **Next**.

   > **NOTE**
   > The **Content** page displays only when the **Detect associated content dependencies and add them to this distribution** setting is selected on the **General** page of the wizard.

6. On the **Content Destination** page, click **Add**, choose one of the following, and then follow the associated step:

   - **Collections**: Select **User Collections** or **Device Collections**, click the collection associated with one or more distribution point groups, and then click **OK**.

     > **NOTE**
     > Only the collections that are associated with a distribution point group are displayed. For more information about associating collections with distribution point groups, see Manage distribution point groups in the Install and configure distribution points for System Center Configuration Manager topic.

- **Distribution Point**: Select an existing distribution point, and then click **OK**. Distribution points that have previously received the content are not displayed.
- **Distribution Point Group**: Select an existing distribution point group, and then click **OK**. Distribution point groups that have previously received the content are not displayed.

When you finish adding content destinations, click **Next**.

7. On the **Summary** page, review the settings for the distribution before you continue. To distribute the content to the selected destinations, click **Next**.
8. The **Progress** page displays the progress of the distribution.
9. The **Confirmation** page displays whether the content was successfully assigned to the points. To monitor the content distribution, see Monitor content you have distributed with System Center Configuration Manager.

Use Prestaged content

You can prestage content files for applications and package types:

- In the Configuration Manager console, you select the content that you need and then use the **Create Prestaged Content File Wizard** to create a compressed, prestaged content file that contains the files and associated metadata for the content that you selected.
- You can then manually import the content at a site server, secondary site, or distribution point.
- When you import the prestaged content file on a site server, the content files are added to the content library on the site server, and then registered in the site server database.
- When you import the prestaged content file on a distribution point, the content files are added to the content library on the distribution point, and a status message is sent to the site server that informs the site that the content is available on the distribution point.

Limitations and considerations for prestaged content:

- **When the distribution point is located on the site server**, do not enable the distribution point for prestaged content. Instead, use the procedure in How to prestage content on a distribution point on a site server.
- **When the distribution point is configured as a pull-distribution point**, do not enable the distribution point for prestaged content. The prestage content configuration for a distribution point overrides the pull-distribution point configuration. A pull-distribution point that is configured for prestaged content does not pull content from source distribution point and does not receive content from the site server.
- **The content library must be created on the distribution point before you can prestage content to the distribution point**. Distribute content over the network at least one time before you prestage content to the distribution point.
- **When you prestage content for a package with a long package source path** (for example, more than 140 characters), the Extract Content command-line tool might fail to successfully extract the content for that package to the content library.

For information about when to prestage content files, see *Prestaged content* in the Manage network bandwidth for content management topic.

Use the following sections to prestage content.

Step 1: Create a Prestaged Content File

You can create a compressed, prestaged content file that contains the files and associated metadata for the content that you select in the Configuration Manager console. Use the following procedure to create a prestaged content file.

To create a prestaged content file

1. In the Configuration Manager console, click **Software Library**.
2. In the **Software Library** workspace, select one of the following steps for the type of content that you want to prestage:
   - **Applications**: Expand **Application Management**, click **Applications**, and then select the applications that you want to prestage.
   - **Packages**: Expand **Application Management**, click **Packages**, and then select the packages that you want to prestage.
   - **Driver Packages**: Expand **Operating Systems**, click **Driver Packages**, and then select the driver packages that you want to prestage.
   - **Operating System Images**: Expand **Operating Systems**, click **Operating System Images**, and then select the operating system images that you want to prestage.
   - **Operating System Installers**: Expand **Operating Systems**, click **Operating System Installers**, and then select the operating system installers that you want to prestage.
   - **Boot Images**: Expand **Operating Systems**, click **Boot Images**, and then select the boot images that you want to prestage.
   - **Task Sequences**: Expand **Operating Systems**, click **Task Sequences**, and then select the task sequence that you want to prestage.
3. On the **Home** tab, in the **Deployment** group, click **Create Prestage Content File**. The Create Prestaged Content File Wizard opens.

   > **NOTE**
   >
   > **For Applications:** On the **Home** tab, in the **Application** group, click **Create Prestaged Content File**.
   >
   > **For Packages:** On the **Home** tab, in the <*PackageName*> group, click **Create Prestaged Content File**.

4. On the **General** page, click **Browse**, choose the location for the prestaged content file, specify a name for the file, and then click **Save**. You use this prestaged content file on primary site servers, secondary site servers, or distribution points to import the content and metadata.
5. For applications, select **Export all dependencies** to have Configuration Manager detect and add the dependencies associated with the application to the prestaged content file. By default, this setting is selected.
6. In **Administrator comments**, enter optional comments about the prestaged content file, and then click **Next**.
7. On the **Content** page, verify that the content listed is the content that you want to add to the prestaged content file, and then click **Next**.
8. On the **Content Locations** page, specify the distribution points from which to retrieve the content files for the prestaged content file. You can select more than one distribution point to retrieve the content. The distribution points are listed in the Content locations section. The **Content** column displays how many of the selected packages or applications are available on each distribution point. Configuration Manager starts with the first distribution point in the list to retrieve the selected content, and then moves down the list in order to retrieve the remaining content required for the prestaged content file. Click **Move Up** or **Move**

Down to change the priority order of the distribution points. When the distribution points in the list do not contain all of the selected content, you must add distribution points to the list that contain the content or exit the wizard, distribute the content to at least one distribution point, and then restart the wizard.

9. On the **Summary** page, confirm the details. You can go back to previous pages and make changes. Click **Next** to create the prestaged content file.
10. The **Progress** page displays the content that is being added to the prestaged content file.
11. On the **Completion** page, verify that the prestaged content file was created successfully, and then click **Close**.

Step 2: Assign the Content to Distribution Points

After you prestage the content file, assign the content to distribution points.

> **NOTE**
> When you use a prestaged content file to recover the content library on a site server, and do not have to prestage the content files on a distribution point, you can skip this procedure.

Use the following procedure to assign the content in the prestaged content file to distribution points.

> **IMPORTANT**
> Verify that the distribution points that you want to prestage are configure as prestaged distribution points, or that the content is distributed to the distribution points by using the network.

To assign the content to distribution points

1. In the Configuration Manager console, click **Software Library**.
2. In the **Software Library** workspace, select one of the following steps for the type of content that you selected when you created the prestaged content file:
   - **Applications**: Expand **Application Management**, click **Applications**, and then select the applications that you prestaged.
   - **Packages**: Expand **Application Management**, click **Packages**, and then select the packages that you prestaged.
   - **Deployment Packages**: Expand **Software Updates**, click **Deployment Packages**, and then select the deployment packages that you prestaged.
   - **Driver Packages**: Expand **Operating Systems**, click **Driver Packages**, and then select the driver packages that you prestaged.
   - **Operating System Images**: Expand **Operating Systems**, click **Operating System Images**, and then select the operating system images that you prestaged.
   - **Operating System Installers**: Expand **Operating Systems**, click **Operating System Installers**, and then select the operating system installers that you prestaged.
   - **Boot Images**: Expand **Operating Systems**, click **Boot Images**, and then select the boot images that you prestaged.
3. On the **Home** tab, in the **Deployment** group, click **Distribute Content**. The Distribute Content Wizard opens.
4. On the **General** page, verify that the content listed is the content that you prestaged, choose whether you

want Configuration Manager to detect content dependencies that are associated with the selected content and add the dependencies to the distribution, and then click **Next**.

> **NOTE**
> You have the option to configure the **Detect associated content dependencies and add them to this distribution** setting only for the application content type. Configuration Manager automatically configures this setting for task sequences, and it cannot be modified.

5. On the **Content** page, if displayed, verify that the content listed is the content that you want to distribute, and then click **Next**.

> **NOTE**
> The **Content** page displays only when the **Detect associated content dependencies and add them to this distribution** setting is selected on the **General** page of the wizard.

6. On the **Content Destination** page, click **Add**, choose one of the following that includes the distribution points to be prestaged, and then follow the associated step:

   - **Collections**: Select **User Collections** or **Device Collections**, click the collection associated with one or more distribution point groups, and then click **OK**.

     > **NOTE**
     > Only the collections that are associated with a distribution point group are displayed. For more information, see Manage distribution point groups in the Install and configure distribution points for System Center Configuration Manager topic.

   - **Distribution Point**: Select an existing distribution point, and then click **OK**. Distribution points that have previously received the content are not displayed.
   - **Distribution Point Group**: Select an existing distribution point group, and then click **OK**. Distribution point groups that have previously received the content are not displayed.

   When you finish adding content destinations, click **Next**.

7. On the **Summary** page, review the settings for the distribution before you continue. To distribute the content to the selected destinations, click **Next**.
8. The **Progress** page displays the progress of the distribution.
9. The **Confirmation** page displays whether or not the content was successfully assigned to the distribution points. To monitor the content distribution, see Monitor content you have distributed with System Center Configuration Manager.

Step 3: Extract the Content from the Prestaged Content File

After you create the prestaged content file and assign the content to distribution points, you can extract the content files to the content library on a site server or distribution point. Typically, you have copied the prestaged content file to a portable drive like a USB drive, or have burned content to media like a DVD, and have it available at the location of the site server or distribution point that requires the content.

Use the following procedure to manually export the content files from the prestaged content file by using the Extract Content command-line tool.

> **IMPORTANT**
>
> When you run the Extract Content command-line tool, the tool creates a temporary file as it creates the prestaged content file. Then, the file is copied to the destination folder and the temporary file is deleted. You must have sufficient disk space for this temporary file or the process fails. The temporary file is created in the following location:
>
> - The temporary file is created in same folder that you specify as the destination folder for the prestaged content file.

> **IMPORTANT**
>
> The user that runs the Extract Content command-line tool must have **Administrator** rights on the computer from which you are extracting the prestaged content.

To extract the content files from the prestaged content file

1. Copy the prestaged content file to the computer from which you want to extract the content.
2. Copy the Extract Content command-line tool from *<ConfigMgrInstallationPath>*\bin*<platform>* to the computer from which you want to extract the prestaged content file.
3. Open the command prompt and navigate to the folder location of the prestaged content file and Extract Content tool.

   > **NOTE**
   >
   > You can extract one or more prestaged content files on a site server, secondary site server, or distribution point.

4. Type **extractcontent /P:***<PrestagedFileLocation>******<PrestagedFileName>* **/S** to import a single file.

   Type **extractcontent /P:***<PrestagedFileLocation>* **/S** to import all prestaged files in the specified folder.

   For example, type **extractcontent /P:D:\PrestagedFiles\MyPrestagedFile.pkgx /S** where `D:\PrestagedFiles\` is the PrestagedFileLocation, `MyPrestagedFile.pkgx` is the prestaged file name, and `/S` informs Configuration Manager to extract only content files that are newer than what is currently on the distribution point.

   When you extract the prestaged content file on a site server, the content files are added to the content library on the site server, and then the content availability is registered in the site server database. When you export the prestaged content file on a distribution point, the content files are added to the content library on the distribution point, the distribution point sends a status message to the parent primary site server, and then the content availability is registered in the site database.

   > **IMPORTANT**
   >
   > In the following scenario, you must update content that you extracted from a prestaged content file when the content is updated to a new version:
   >
   > 1. You create a prestaged content file for version 1 of a package.
   > 2. You update the source files for the package with version 2.
   > 3. You extract the prestaged content file (version 1 of the package) on a distribution point.
   >
   > Configuration Manager does not automatically distribute package version 2 to the distribution point. You must create a new prestaged content file that contains the new file version and then extract the content, update the distribution point to distribute the files that have changed, or redistribute all files in the package.

How to prestage content on a distribution point on a site server

When a distribution point is installed on a site server, you must use the following procedure to successfully prestage content. This is because the content files are already in the content library.

When the distribution point is not enabled for prestage content or when the distribution point is not located on a site server, see the Use Prestaged content section in this topic.

To prestage content on distribution points located on a site server

1. Use the following steps to verify that the distribution point is not enabled for prestaged content.
    a. In the Configuration Manager console, click **Administration**.
    b. In the **Administration** workspace, click **Distribution Points**, and then select the distribution point that is located on the site server.
    c. On the **Home** tab, in the **Properties** group, click **Properties**.
    d. On the **General** tab, verify that the **Enable this distribution point for prestaged content** check box is not selected.
2. Create the prestaged content file by using the Step 1: Create a Prestaged Content File section in this topic.
3. Assign the content to the distribution point by using the Step 2: Assign the Content to Distribution Points section in this topic.
4. On the site server, extract the content from the prestaged content file by using the Step 3: Extract the Content from the Prestaged Content File section in this topic.

> **NOTE**
> When the distribution point is on a secondary site, wait for at least 10 minutes, and then by using a Configuration Manager console that is connected to the parent primary site, assign the content to the distribution point on the secondary site.

Manage the content you have distributed

You have the following options for managing content:

- Update content
- Redistribute content
- Remove content
- validate content

Update content

When the source file location for a deployment is updated by adding new files or replace existing files with a newer version, you can update the content files on distribution points by using the **Update Distribution Points** or **Update Content** action:

- The content files are copied from the source file path to the content library on the site that owns the package content source
- The package version is incremented
- Each instance of the content library on site servers and on distribution points updates with only the files that have changed

> **WARNING**
> The package version for applications is always 1. When you update the content for an application deployment type, Configuration Manager creates a new content ID for the deployment type, and the package references the new content ID.

To update content on distribution points

1. In the Configuration Manager console, click **Software Library**.
2. In the **Software Library** workspace, select one of the following steps for the type of content that you want to distribute:
   - **Applications**: Expand **Application Management** > **Applications**, and then select the applications that you want to distribute. Click the **Deployment Types** tab, and then select the deployment type that you want to update.
   - **Packages**: Expand **Application Management** > **Packages**, and then select the packages that you want to update.
   - **Deployment Packages**: Expand **Software Updates** > **Deployment Packages**, and then select the deployment packages that you want to update.
   - **Driver Packages**: Expand **Operating Systems** > **Driver Packages**, and then select the driver packages that you want to update.
   - **Operating System Images**: Expand **Operating Systems** > **Operating System Images**, and then select the operating system images that you want to update.
   - **Operating System Installers**: Expand **Operating Systems** > **Operating System Installers**, and then select the operating system installers that you want to update.
   - **Boot Images**: Expand **Operating Systems** > **Boot Images**, and then select the boot images that you want to update.
3. On the **Home** tab, in the **Deployment** group, click **Update Distribution Points**, and then click **OK** to confirm that you want to update the content.

> **NOTE**
> To update content for applications, click the **Deployment Types** tab, right-click the deployment type, click **Update Content**, and then click **OK** to confirm that you want to refresh the content.

> **NOTE**
> When you update content for boot images, the Manage Distribution Point Wizard opens. Review the information on the **Summary** page, and then complete the wizard to update the content.

Redistribute content

You can redistribute a package to copy all of the content files in the package to distribution points or distribution point groups and thereby overwrite the existing files.

Use this operation to repair content files in the package or resend the content when the initial distribution fails. You can redistribute a package from:

- Package properties
- Distribution point properties

- Distribution point group properties.

To redistribute content from package properties

1. In the Configuration Manager console, click **Software Library**.
2. In the **Software Library** workspace, select one of the following steps for the type of content that you want to distribute:
   - **Applications**: Expand **Application Management** > **Applications**, and then select the application that you want to redistribute.
   - **Packages**: Expand **Application Management** > **Packages**, and then select the package that you want to redistribute.
   - **Deployment Packages**: Expand **Software Updates** > **Deployment Packages**, and then select the deployment package that you want to redistribute.
   - **Driver Packages**: Expand **Operating Systems** > **Driver Packages**, and then select the driver package that you want to redistribute.
   - **Operating System Images**: Expand **Operating Systems** > **Operating System Images**, and then select the operating system image that you want to redistribute.
   - **Operating System Installers**: Expand **Operating Systems** > **Operating System Installers**, and then select the operating system installer that you want to redistribute.
   - **Boot Images**: Expand **Operating Systems** > **Boot Images**, and then select the boot image that you want to redistribute.
3. On the **Home** tab, in the **Properties** group, click **Properties**.
4. Click the **Content Locations** tab, select the distribution point or distribution point group in which you want to redistribute the content, click **Redistribute**, and then click **OK**.

To redistribute content from distribution point properties

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, click **Distribution Points**, and then select the distribution point in which you want to redistribute content.
3. On the **Home** tab, in the **Properties** group, click **Properties**.
4. Click the **Content** tab, select the content to redistribute, click **Redistribute**, and then click **OK**.

To redistribute content from distribution point group properties

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, click **Distribution Point Groups**, and then select the distribution point group in which you want to redistribute content.
3. On the **Home** tab, in the **Properties** group, click **Properties**.
4. Click the **Content** tab, select the content to redistribute, click **Redistribute**, and then click **OK**.

> **IMPORTANT**
> The content in the package is redistributed to all of the distribution points in the distribution point group.

Use the SDK to force replication of content

You can use the **RetryContentReplication** Windows Management Instrumentation (WMI) class method from the

Configuration Manager SDK to force Distribution Manager to copy content from the source location to the content library.

Only use this method to force replication when you must redistribute content after there were issues with normal replication of content (typically confirmed by use of the Monitoring node of the console).

For more information about this SDK option, see RetryContentReplication Method in Class SMS_CM_UpdatePackages on MSDN.Microsoft.com.

Remove content

When you no longer require content on your distribution points, you can remove the content files on the distribution point.

- Package properties
- Distribution point properties
- Distribution point group properties.

However, when the content is associated with another package that was distributed to the same distribution point, you cannot remove the content.

To remove package content files from distribution points

1. In the Configuration Manager console, click **Software Library**.
2. In the **Software Library** workspace, select one of the following steps for the type of content that you want to delete:
   - **Applications**: Expand **Application Management** > **Applications**, and then select the application that you want to remove.
   - **Packages**: Expand **Application Management** > **Packages**, and then select the package that you want to remove.
   - **Deployment Packages**: Expand **Software Updates** > **Deployment Packages**, and then select the deployment package that you want to remove.
   - **Driver Packages**: Expand **Operating Systems** > **Driver Packages**, and then select the driver package that you want to remove.
   - **Operating System Images**: Expand **Operating Systems** > **Operating System Images**, and then select the operating system image that you want to remove.
   - **Operating System Installers**: Expand **Operating Systems** > **Operating System Installers**, and then select the operating system installer that you want to remove.
   - **Boot Images**: Expand **Operating Systems** > **Boot Images**, and then select the boot image that you want to remove.
3. On the **Home** tab, in the **Properties** group, click **Properties**.
4. Click the **Content Locations** tab, select the distribution point or distribution point group from which you want to remove the content, click **Remove**, and then click **OK**.

To remove package content from distribution point properties

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, click **Distribution Points**, and then select the distribution point in which you want to delete the content.
3. On the **Home** tab, in the **Properties** group, click **Properties**.

4. Click the **Content** tab, select the content to remove, click **Remove**, and then click **OK**.

To remove content from distribution point group properties

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, click **Distribution Point Groups**, and then select the distribution point group in which you want to remove content.
3. On the **Home** tab, in the **Properties** group, click **Properties**.
4. Click the **Content** tab, select the content to remove, click **Remove**, and then click **OK**.

Validate content

The content validation process verifies the integrity of content files on distribution points. You enable content validation on a schedule, or you can manually initiate content validation from the properties of distribution points and packages.

When the content validation process starts, Configuration Manager verifies the content files on distribution points, and if the file hash is unexpected for the files on the distribution point, Configuration Manager creates a status message that you can review in the **Monitoring** workspace.

For more information about configuring the content validation schedule, see Distribution point configurations in the Install and configure distribution points for System Center Configuration Manager topic.

To initiate content validation for all content on a distribution point

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, click **Distribution Points**, and then select the distribution point in which you want to validate content.
3. On the **Home** tab, in the **Properties** group, click **Properties**.
4. On the **Content** tab, select the package in which you want to validate the content, click **Validate**, click **OK**, and then click **OK**. The content validation process initiates for the package on the distribution point.
5. To view the results of the content validation process, in the **Monitoring** workspace, expand **Distribution Status**, and click the **Content Status** node. The content for each package type (for example, Application, Software Update Package, and Boot Image) is displayed. For more information about monitoring content status, see Monitor content you have distributed with System Center Configuration Manager.

To initiate content validation for a package

1. In the Configuration Manager console, click **Software Library**.
2. In the **Software Library** workspace, select one of the following steps for the type of content that you want to validate:
   - **Applications**: Expand **Application Management** > **Applications**, and then select the application that you want to validate.
   - **Packages**: Expand **Application Management** > **Packages**, and then select the package that you want to validate.
   - **Deployment Packages**: Expand **Software Updates** > **Deployment Packages**, and then select the deployment package that you want to validate.
   - **Driver Packages**: Expand **Operating Systems** > **Driver Packages**, and then select the driver package that you want to validate.
   - **Operating System Images**: Expand **Operating Systems** > **Operating System Images**, and then select the operating system image that you want to validate.

- **Operating System Installers**: Expand **Operating Systems** > **Operating System Installers**, and then select the operating system installer that you want to validate.
- **Boot Images**: Expand **Operating Systems** > **Boot Images**, and then select the boot image that you want to prestage.

3. On the **Home** tab, in the **Properties** group, click **Properties**.
4. On the **Content Locations** tab, select the distribution point or distribution point group in which to validate the content, click **Validate**, click **OK**, and then click **OK**. The content validation process starts for the content on the selected distribution point or distribution point group.
5. To view the results of the content validation process, in the **Monitoring** workspace, expand **Distribution Status**, and click the **Content Status** node. The content for each package type (for example, Application, Software Update Package, and Boot Image) is displayed. For more information about monitoring the content status, see Monitor content you have distributed with System Center Configuration Manager.

Monitor content you distribute with Configuration Manager

7/26/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the Configuration Manager console to monitor distributed content, including:

- The status for all package types for the associated distribution points.
- The content validation status for the content in a package.
- The status of content assigned to a specific distribution point group.
- The state of content assigned to a distribution point.
- The status of optional features for each distribution point (content validation, PXE, and multicast).

> **NOTE**
> Configuration Manager only monitors the content on a distribution point that's in the content library. It doesn't monitor content stored on the distribution point in package or custom shares.

Content status monitoring

The **Content Status** node in the **Monitoring** workspace provides information about content packages. In the Configuration Manager console, review information like:

- Package name, type, and ID
- How many distribution points a package has been sent to
- Compliance rate
- When the package was created
- Source version

You also find detailed status information for any package, including:

- Distribution status
- The number of failures
- Pending distributions
- The number of installations

You can also manage distributions that remain in progress to a distribution point, or that failed to successfully distribute content to a distribution point:

- The option to either cancel or redistribute content is available when you view the deployment status message of a distribution job to a distribution point in the **Asset Details** pane. This pane can be found in either the **In Progress** tab or the **Error** tab of the **Content Status** node.
- Additionally, the job details display the percentage of the job that has completed when you view the details of a job on the **In Progress** tab. The job details also display the number of retries that remain for a job. When you view the details of a job on the **Error** tab, it shows how long before the next retry occurs.

When you cancel a deployment that's not yet complete, the distribution job to transfer that content stops:

- The status of the deployment then updates to indicate that the distribution failed, and that it was canceled by a

user action.

- This new status appears in the **Error** tab.

> **NOTE**
>
> When a deployment is near completion, it's possible the action to cancel that distribution won't process before the distribution to the distribution point completes. When this occurs, the action to cancel the deployment is ignored, and the status for the deployment displays as successful.
>
> Although you can select the option to cancel a distribution to a distribution point that is located on a site server, this has no effect. This behavior is because the site server and the distribution point on a site server share the same single instance content store. There's no actual distribution job to cancel.

When you redistribute content that previously failed to transfer to a distribution point, Configuration Manager immediately begins redeploying that content to the distribution point. Configuration Manager updates the status of the deployment to reflect the ongoing state of that redeployment.

Tasks to monitor content

1. In the Configuration Manager console, go to the **Monitoring** workspace, expand **Distribution Status**, and then select the **Content Status** node. This node displays the packages.
2. Select the package you want to manage.
3. On the **Home** tab of the ribbon, in the **Content** group, select **View Status**. The console displays detailed status information for the package.

Continue to one of the following sections for additional actions:

Cancel a distribution that remains in progress

1. Switch to the **In Progress** tab.
2. In the **Asset Details** pane, right-click the entry for the distribution that you want to cancel, and select **Cancel**.
3. Select **Yes** to confirm the action and cancel the distribution job to that distribution point.

Redistribute content that failed to distribute

1. Switch to the **Error** tab.
2. In the **Asset Details** pane, right-click the entry for the distribution that you want to redistribute, and select **Redistribute**.
3. Select **Yes** to confirm the action and start the redistribution process to that distribution point.

Distribution point group status

The **Distribution Point Group Status** node in the **Monitoring** workspace provides information about distribution point groups. You can review information like:

- The distribution point group name, description, and status
- How many distribution points are members of the distribution point group
- How many packages have been assigned to the group
- The compliance rate

You also view the following detailed status information:

- Errors for the distribution point group
- How many distributions are in progress

- How many have been successfully distributed

Monitor distribution point group status

1. In the Configuration Manager console, go to the **Monitoring** workspace, expand **Distribution Status**, and then select the **Distribution Point Group Status** node. It displays the distribution point groups.
2. Select the distribution point group for which you want detailed status information.
3. On the **Home** tab of the ribbon, select **View Status**. It displays detailed status information for the distribution point group.

Distribution point configuration status

The **Distribution Point Configuration Status** node in the **Monitoring** workspace provides information about the distribution point. You can review what attributes are enabled for the distribution point, such as the PXE, multicast, content validation. Also review the distribution status for the distribution point.

> **WARNING**
> Distribution point configuration status is relative to the last 24 hours. If the distribution point has an error and recovers, the error status might be displayed for up to 24 hours after the distribution point recovers.

Monitor distribution point configuration status

1. In the Configuration Manager console, go to the **Monitoring** workspace, expand **Distribution Status**, and then select the **Distribution Point Configuration Status** node.
2. Select a distribution point.
3. In the results pane, switch to the **Details** tab. It displays status information for the distribution point.

Client Data Sources dashboard

Use the **Client Data Sources** dashboard to better understand from where clients get content in your environment. The dashboard starts displaying data after clients download content and report that information back to the site. This process can take up to 24 hours.

> **NOTE**
> Configuration Manager doesn't enable this optional feature by default. You must enable the **Client Peer Cache** feature before using it. For more information, see Enable optional features from updates.

In the Configuration Manager console, go to the **Monitoring** workspace, expand **Distribution Status**, and select the **Client Data Sources** node. Select a time period to apply to the dashboard. Then select the boundary group for which you want to view information. You can hover your mouse over tiles to see more details about the different content or policy sources.

Also use the report, **Client Data Sources - Summarization**, to view a summary of the client data sources for each boundary group.

Dashboard tiles

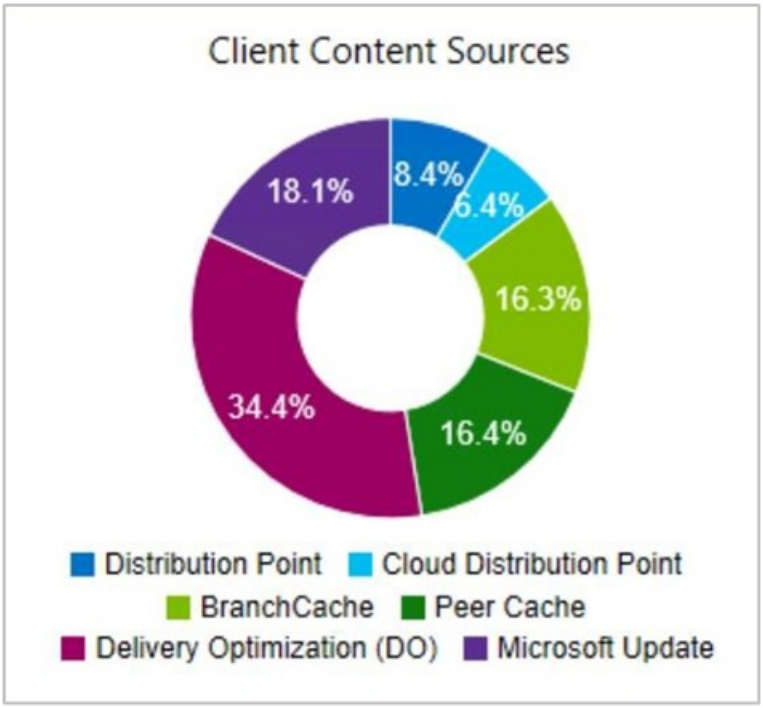
The dashboard includes the following tiles:

Client Content Sources

Displays the sources from which clients got content:

- Distribution point

- Cloud distribution point
- BranchCache
- Peer Cache
- Delivery Optimization (starting in version 1906)[Note 1]
- Microsoft Update: Devices report this source when the Configuration Manager client downloads software updates from Microsoft cloud services. These services include Microsoft Update and Office 365.



> **NOTE**
>
> Starting in version 1906, to include Delivery Optimization on this dashboard, do the following actions:
>
> - Configure the client setting, **Enable installation of Express Updates on clients** in the Software Updates group
> - Deploy Windows 10 express updates
>
> For more information, see Manage Express installation files for Windows 10 updates.

Distribution points

Displays the number of distribution points that are part of the selected boundary group.

Clients that used a distribution point

Of the number of clients that are in the selected boundary group, this tile shows how many used a distribution point to get content.

Peer Cache sources

For the selected boundary group, this tile shows how many peer cache sources have reported download history.

Clients that used a peer

Of the number of clients that are in the selected boundary group, this tile shows how many used a peer cache source to get content.

Top Distributed Content

The most distributed packages by source type

Delivery Optimization In-Network Cache in Configuration Manager

9/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Starting in version 1906, you can install a Delivery Optimization In-Network Cache (DOINC) server on your distribution points. By caching this content on-premises, your clients can benefit from the Delivery Optimization feature, but you can help to protect WAN links.

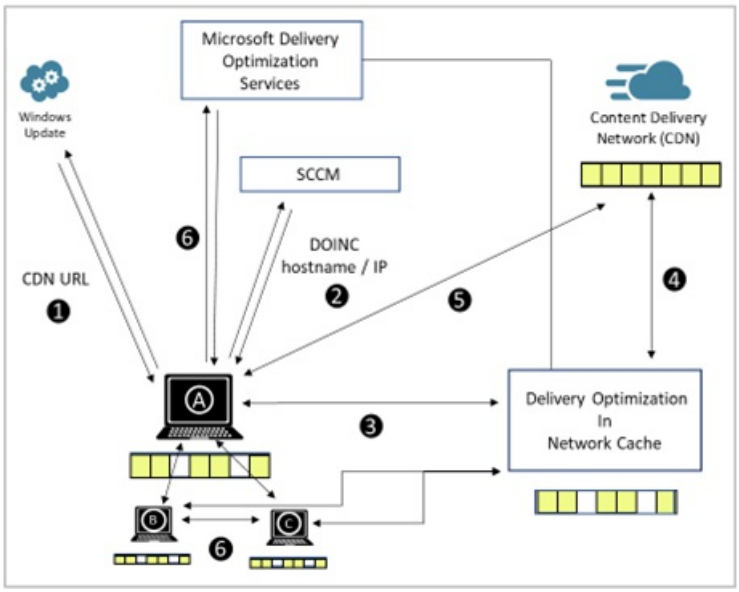
This cache server acts as an on-demand transparent cache for content downloaded by Delivery Optimization. Use client settings to make sure this server is offered only to the members of the local Configuration Manager boundary group.

This cache is separate from Configuration Manager's distribution point content. If you choose the same drive as the distribution point role, it stores content separately.

> **NOTE**
> Delivery Optimization In-Network Cache server is an application installed on Windows Server that's still in development. It's tagged with a *beta* label in the Configuration Manager console.

How it works

When you configure clients to use the Delivery Optimization In-Network Cache server, they no longer request Microsoft cloud-managed content from the internet. Clients request this content from the DOINC server installed on the distribution point. The DOINC server caches this content using the IIS feature for Application Request Routing (ARR). Then the cache server can quickly respond to any future requests for the same content. If the DOINC server is unavailable, or the content isn't yet cached, clients download the content from the internet. Clients also use Delivery Optimization, so download portions of the content from peers in their network.



1. Client checks for updates and gets the address for the content delivery network (CDN).
2. Configuration Manager configures Delivery Optimization (DO) settings on the client, including the cache

server name.

3. Client A requests content from the DO cache server.
4. If the cache doesn't include the content, then the DO cache server gets it from the CDN.
5. If the cache server fails to respond, the client downloads the content from the CDN.
6. Clients use DO to get pieces of the content from peers.

Prerequisites and limitations

- An *on-premises* distribution point, with the following configurations:
  - Running Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019
  - The default web site enabled on port 80
  - Don't preinstall the IIS Application Request Routing (ARR) feature. DOINC installs ARR and configures its settings. Microsoft can't guarantee that DOINC's ARR configuration won't conflict with other applications on the server that also use this feature.
  - The distribution point requires internet access to the Microsoft cloud. The specific URLs can vary depending upon the specific cloud-enabled content. For more information, see Internet access requirements.
- Clients running Windows 10 version 1709 or later

Enable DOINC

1. In the Configuration Manager console, go to the **Administration** workspace, and select the **Distribution Points** node.
2. Select an on-premises distribution point, and then in the ribbon select **Properties**.
3. In the properties of the distribution point role, on the **General** tab, configure the following settings:
   a. Enable the option to **Enable this distribution point to be used as Delivery Optimization In-Network Cache server**

      View and accept the license terms.

   b. **Local drive to be used**: Select the disk to use for the cache. **Automatic** is the default value, which uses the disk with the most free space.[Note 1]

      > **NOTE**
      > You can change this drive later. Any cached content is lost, unless you copy it to the new drive.

   c. **Disk space**: Select the amount of disk space to reserve in GB or a percentage of the total disk space. By default, this value is 100 GB.

      > **NOTE**
      > The default cache size should be sufficient for most customers. You can adjust the cache size later.

   d. **Retain cache when disabling the in-network cache server**: If you remove the cache server, and

you enable this option, the server keeps the cache's content on the disk.

4. In client settings, in the **Delivery Optimization** group, configure the setting to **Enable devices managed by Configuration Manager to use Delivery Optimization In-Network Cache servers (Beta) for content download**.

Note 1: About drive selection

If you select **Automatic**, when Configuration Manager installs the DOINC component, it honors the **no_sms_on_drive.sms** file. For example, the distribution point has the file `C:\no_sms_on_drive.sms`. Even if the C: drive has the most free space, Configuration Manager configures DOINC to use another drive for its cache.

If you select a specific drive that already has the **no_sms_on_drive.sms** file, Configuration Manager ignores the file. Configuring DOINC to use that drive is an explicit intent. For example, the distribution point has the file `F:\no_sms_on_drive.sms`. When you explicitly configure the distribution point properties to use the **F:** drive, Configuration Manager configures DOINC to use the F: drive for its cache.

To change the drive after DOINC is installed:

- Manually configure the distribution point properties to use a specific drive letter.
- If set to automatic, first create the **no_sms_on_drive.sms** file. Then make some change to the distribution point properties to trigger a configuration change.

Verify

When clients download cloud-managed content, they use Delivery Optimization from the cache server installed on your distribution point. Cloud-managed content includes the following types:

- Microsoft Store apps
- Windows features on demand, such as languages
- If you enable Windows Update for Business policies: Windows 10 feature and quality updates
- For co-management workloads:
  - Windows Update for Business: Windows 10 feature and quality updates
  - Office Click-to-Run apps: Office apps and updates
  - Client apps: Microsoft Store apps and updates
  - Endpoint Protection: Windows Defender definition updates

On Windows 10 version 1809 or later, verify this behavior with the **Get-DeliveryOptimizationStatus** Windows PowerShell cmdlet. In the cmdlet output, review the **BytesFromCacheServer** value. For more information, see Monitor Delivery Optimization.

If the cache server returns any HTTP failure, the Delivery Optimization client falls back to the original cloud source.

For more detailed information, see Troubleshoot Delivery Optimization In-Network Cache in Configuration Manager.

See also

Optimize Windows 10 updates with Delivery Optimization

Troubleshoot Delivery Optimization In-Network Cache in Configuration Manager

Troubleshoot Delivery Optimization In-Network Cache in Configuration Manager

9/11/2019 • 5 minutes to read • Edit Online

This article provides technical details about Delivery Optimization In-Network Cache (DOINC) in Configuration Manager. It's to help you troubleshoot issues that you may have in your environment. For more information on how it works and how to use it, see Delivery Optimization In-Network Cache in Configuration Manager.

Verify

When you correctly install the Delivery Optimization cache server, and correctly configure clients, they download from the cache server installed on your distribution point rather than the internet.

Verify this behavior on a client or on the server.

Verify on a client

1. On client running Windows 10, version 1809 or later, download cloud-managed content. For more information on the types of content that DOINC supports, see Verify DOINC.
2. Open PowerShell and run the following command: `Get-DeliveryOptimizationStatus`

For example:

```
PS C:\> Get-DeliveryOptimizationStatus

FileId                      : ec523d49c4f7c3c4444f0d9b952286ce40fdcee4
FileSize                    : 549064
TotalBytesDownloaded        : 549064
PercentPeerCaching          : 0
BytesFromPeers              : 0
BytesFromHttp               : 0
Status                      : Caching
Priority                    : Background
BytesFromCacheServer        : 549064
BytesFromLanPeers           : 0
BytesFromGroupPeers         : 0
BytesFromInternetPeers      : 0
BytesToLanPeers             : 0
BytesToGroupPeers           : 0
BytesToInternetPeers        : 0
DownloadDuration            : 00:00:00.0780000
HttpConnectionCount         : 2
LanConnectionCount          : 0
GroupConnectionCount        : 0
InternetConnectionCount     : 0
DownloadMode                : 99
SourceURL                   :
http://au.download.windowsupdate.com/c/msdownload/update/software/defu/2019/09/am_delta_p
                              atch_1.301.664.0_ec523d49c4f7c3c4444f0d9b952286ce40fdcee4.exe
NumPeers                    : 0
PredefinedCallerApplication : WU Client Download
ExpireOn                    : 9/6/2019 8:36:19 AM
IsPinned                    : False
```

Notice that the `BytesFromCacheServer` attribute isn't zero.

If the client isn't configured correctly, or the cache server isn't installed correctly, the Delivery Optimization client falls back to the original cloud source. Then the BytesFromCacheServer attribute will be zero.

Verify on the server

First, verify the registry properties are configured correctly: `HKLM\SOFTWARE\Microsoft\Delivery Optimization In-Network Cache`. For example, the drive cache location is `PrimaryDrivesInput\DOINC-E77D08D0-5FEA-4315-8C95-10D359D59294`, where `PrimaryDrivesInput` can be multiple drives such as `C,D,E`.

Next, use the following method to simulate a client download request to the server with the mandatory headers.

1. Open a 64-bit PowerShell window as an administrator.
2. Run the following command, and replace the name or IP address of your server for `<DoincServer>`:

```
Invoke-WebRequest -URI "http://<DoincServer>/mscomtest/wuidt.gif" -Headers
@{"Host"="b1.download.windowsupdate.com"}
```

The output looks similar to the following example:

```
PS C:\WINDOWS\system32> Invoke-WebRequest -URI "http://SERVER01.CONTOSO.COM/mscomtest/wuidt.gif" -Headers
@{"Host"="b1.download.windowsupdate.com"}


StatusCode        : 200
StatusDescription : OK
Content           : {71, 73, 70, 56...}
RawContent        : HTTP/1.1 200 OK
                    X-HW:
1567797125.dop019.se2.t,1567797125.cds058.se2.s,1567797125.dop114.at2.r,1567797125.cds079.at2
                    .p,1567797125.cds058.se2.p
                    X-CCC: cdP+dRBgUCoZO1mezA9zhg2VwQ7P1JWTh9k+GhfQmu8=_SLwv...
Headers           : {[X-HW,
1567797125.dop019.se2.t,1567797125.cds058.se2.s,1567797125.dop114.at2.r,1567797125.cds079.a
                    t2.p,1567797125.cds058.se2.p], [X-CCC,
                    cdP+dRBgUCoZO1mezA9zhg2VwQ7P1JWTh9k+GhfQmu8=_SLwvtSBQdT3uPQ5ikBe1ABMbdYIIncem+h5dtcLI6GY=],
                    [X-CID, 100], [Accept-Ranges, bytes]...}
RawContentLength  : 969710
```

The following attributes indicate success:

- `StatusCode : 200`
- `StatusDescription : OK`

Log files

- ARR setup log: `%temp%\arr_setup.log`
- DO cache server setup log: `SMS_DP$\Ms.Dsp.Do.Inc.Setup\DoincSetup.log` on the distribution point, and `DistMgr.log` on the site server
- IIS operational logs: By default, `%SystemDrive%\inetpub\logs\LogFiles`
- DO cache server operational log: `C:\Doinc\Product\Install\Logs`

> **TIP**
> Among other uses, this log can help you identify connectivity issues with the Microsoft cloud.

Setup error codes

When Configuration Manager installs the DOINC component on the distribution point, the following table lists the possible error codes that might occur:

ERROR CODE	ERROR DESCRIPTION
0x00000000	Success
0x00000BC2	Success, reboot required
0x00000643	Generic install failure
0x00D00001	DOINC setup can only be run if Internet Information Services (IIS) has been installed
0x00D00002	DOINC setup can only be run if a 'Default Web Site' exists on the server
0x00D00003	You can't install DOINC if Application Request Routing (ARR) is already installed
0x00D00004	DOINC setup can only be run if Application Request Routing (ARR) was installed by the Install.ps1 script
0x00D00005	DOINC setup requires a PowerShell session running as Administrator
0x00D00006	DOINC setup can only be run from a 64-bit PowerShell environment
0x00D00007	DOINC setup can only be run on a Windows Server
0x00D00008	Failure: The number of cache drives specified must match the number of cache drive size percentages specified
0x00D00009	Failure: A valid cache node ID must be supplied
0x00D0000A	Failure: A valid cache drive set must be supplied
0x00D0000B	Failure: A valid cache drive size percent set must be supplied
0x00D0000C	Failure: A valid cache drive size percent set or cache drive size in GB must be supplied
0x00D0000D	Failure: A valid cache drive size percent set and cache drive size in GB cannot both be supplied
0x00D0000E	Failure: The number of cache drives specified must match the number of cache drive size in GB specified
0x00D0000F	Failure: Couldn't back up the applicationhost.config file from $AppHostConfig to $AppHostConfigDestinationName

ERROR CODE	ERROR DESCRIPTION
0x00D00010	Failure: Couldn't back up the Default Web Site web.config file from $WebsiteConfigFilePath to $WebConfigDestinationName
0x00D00011	Failure: An exception occurred in SetupARRWebFarm.ps1
0x00D00012	Failure: An exception occurred in SetupARRWebFarmRewriteRules.ps1
0x00D00013	Failure: An exception occurred in SetupARRWebFarmProperties.ps1
0x00D00014	Failure: An exception occurred in SetupAllowableServerVariables.ps1
0x00D00015	Failure: An exception occurred in SetupFirewallRules.ps1
0x00D00016	Failure: An exception occurred in SetupAppPoolProperties.ps1
0x00D00017	Failure: An exception occurred in SetupARROutboundRules.ps1
0x00D00018	Failure: An exception occurred in SetupARRDiskCache.ps1
0x00D00019	Failure: An exception occurred in SetupARRProperties.ps1
0x00D0001A	Failure: An exception occurred in SetupARRHealthProbes.ps1
0x00D0001B	Failure: An exception occurred in VerifyIISSItesStarted.ps1
0x00D0001C	Failure: An exception occurred in SetDrivesToHealthy.ps1
0x00D0001D	Failure: An exception occurred in VerifyCacheNodeSetup.ps1
0x00D0001E	You can't install DOINC if the Default Web Site isn't on port 80
0x00D0001F	Failure: The cache drive allocation in percentage can't exceed 100
0x00D00020	Failure: The cache drive allocation in GB cannot exceed the drive's free space
0x00D00021	Failure: The cache drive allocation in percentage must be greater than 0
0x00D00022	Failure: The cache drive allocation in GB must be greater than 0
0x00D00023	Failure: An exception occurred in RegisterScheduledTask_CacheNodeKeepAlive
0x00D00024	Failure: An exception occurred in RegisterScheduledTask_Maintenance

ERROR CODE	ERROR DESCRIPTION
0x00D00025	Failure: An exception occurred setting up the rewrite rules for HTTPS farm: $FarmName
0x00D00026	Failure: An exception occurred setting up the rewrite rules for HTTP farm: $FarmName
0x00D00027	You can't install DOINC because dependent software "Application Request Routing (ARR)" failed to install. See the log file located at %temp%\arr_setup.log

IIS configurations

The DO cache server install makes several modifications to the IIS configuration on the distribution point.

Application request routing

The DO cache server installs and configures IIS Application Request Routing (ARR). To avoid potential conflicts, the distribution point can't already have this component installed.

Allowed server variables

After you install the DO cache server, the default web site has the following *local* server variables:

- HTTP_HOST
- QUERY_STRING
- X-CCC
- X-CID
- X-DOINC-OUTBOUND

Rewrite rules

The DO cache server adds the following rewrite rules:

Inbound rewrite rules

- `Doinc_ForwardToFarm_shswda01.download.manage-selfhost.microsoft.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_swdc01.manage.microsoft.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_swdc02.manage.microsoft.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_dl.delivery.mp.microsoft.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_officecdn.microsoft.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_b1.download.windowsupdate.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_download.windowsupdate.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_officecdn.microsoft.com.edgesuite.net_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_au.b1.download.windowsupdate.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_assets1.xboxlive.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_au.download.windowsupdate.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_emdl.ws.microsoft.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_tlu.dl.delivery.mp.microsoft.com_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_ForwardToFarm_assets2.xboxlive.com_E77D08D0-5FEA-4315-8C95-10D359D59294`

Outbound rewrite rules

- `Doinc_Outbound_SetHeader_X_CID_E77D08D0-5FEA-4315-8C95-10D359D59294`
- `Doinc_Outbound_SetHeader_X_CCC_E77D08D0-5FEA-4315-8C95-10D359D59294`

Manage server resources

Disk space required for each DO cache server may vary, based on your organization's update requirements. 100 GB should be enough space to cache the following content:

- A feature update
- Two to three months of quality and Office updates
- Microsoft Intune apps and Windows inbox apps

The DO cache server shouldn't consume much system memory or processor time. After you install the DO cache server, if you notice significant process or memory resource consumption, analyze the IIS and ARR log files.

If the IIS and ARR log files take up too much space on the server, there are several methods you can use to manage the log files. For more information, see Managing IIS Log File Storage.

See also

Delivery Optimization In-Network Cache in Configuration Manager

Run discovery for System Center Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You use one or more discovery methods in System Center Configuration Manager to find device and user resources that you can manage. You can also use discovery to identify network infrastructure in your environment. There are several different methods you can use to discover different things, and each method has its own configurations and limitations.

Overview of discovery

Discovery is the process by which Configuration Manager learns about the things you can manage. The following are the available discovery methods:

- Active Directory Forest Discovery
- Active Directory Group Discovery
- Active Directory System Discovery
- Active Directory User Discovery
- Heartbeat Discovery
- Network Discovery
- Server Discovery

> **TIP**
>
> You can learn about the individual discovery methods in About discovery methods for System Center Configuration Manager.
>
> For assistance in selecting which methods to use, and at which sites in your hierarchy, see Select discovery methods to use for System Center Configuration Manager.

To use most discovery methods, you must enable the method at a site, and set it up to search specific network or Active Directory locations. When it runs, it queries the specified location for information about devices or users that Configuration Manager can manage. When a discovery method successfully finds information about a resource, it puts that information into a file called a discovery data record (DDR). That file is then processed by a primary or central administration site. Processing of a DDR creates a new record in the site database for newly discovered resources, or updates existing records with new information.

Some discovery methods can generate a large volume of network traffic, and the DDRs they produce can result in a significant use of CPU resources during processing. Therefore, plan to use only those discovery methods that you require to meet your goals. You might start by using only one or two discovery methods, and then later enable additional methods in a controlled manner to extend the level of discovery in your environment.

After discovery information is added to the site database, the information then replicates to each site in the hierarchy, regardless of where it was discovered or processed. Therefore, while you can set up different schedules and settings for discovery methods at different sites, you might run a specific discovery method at only a single

site. This reduces the use of network bandwidth through duplicate discovery actions, and reduces the processing of redundant discovery data at multiple sites.

You can use discovery data to create custom collections and queries that logically group resources for management tasks. For example:

- Pushing client installations, or upgrading.
- Deploying content to users or devices.
- Deploying client settings and related configurations.

About discovery data records

DDRs are files created by a discovery method. They contain information about a resource you can manage in Configuration Manager, such as computers, users, and in some cases, network infrastructure. They are processed at primary sites or at central administration sites. After the resource information in the DDR is entered into the database, the DDR is deleted, and the information replicates as global data to all sites in the hierarchy.

The site at which a DDR is processed depends on the information it contains:

- DDRs for newly discovered resources that are not in the database are processed at the top-level site of the hierarchy. The top-level site creates a new resource record in the database, and assigns it a unique identifier. DDRs transfer by file-based replication until they reach the top-level site.
- DDRs for previously discovered objects are processed at primary sites. Child primary sites do not transfer DDRs to the central administration site when the DDR contains information about a resource that is already in the database.
- Secondary sites do not process DDRs, and always transfer them by file-based replication to their parent primary site.

DDR files are identified by the .ddr extension, and have a typical size of about 1 KB.

Get started with discovery:

Before using the Configuration Manager console to set up discovery, you should understand the differences among the methods, what they can do, and for some, their limitations.

The following topics can build a foundation that will help you use discovery methods successfully:

- About discovery methods for System Center Configuration Manager
- Select discovery methods to use for System Center Configuration Manager

Then, when you understand the methods you want to use, find guidance to set up each method in Configure discovery methods for System Center Configuration Manager.

About discovery methods for System Center Configuration Manager

8/8/2019 • 25 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager discovery methods find different devices on your network, devices and users from Active Directory, or users from Azure Active Directory (Azure AD). To efficiently use a discovery method, you should understand its available configurations and limitations.

Active Directory Forest Discovery

Configurable: Yes

Enabled by default: No

Accounts you can use to run this method:

- **Active Directory Forest Discovery Account** (user defined)
- **Computer account** of the site server

Unlike other Active Directory discovery methods, Active Directory Forest Discovery does not discover resources that you can manage. Instead, this method discovers network locations that are configured in Active Directory. It can convert those locations into boundaries for use throughout your hierarchy.

When this method runs, it searches the local Active Directory forest, each trusted forest, and each additional forest that you configure in the **Active Directory Forests** node of the Configuration Manager console.

Use Active Directory Forest Discovery to:

- Discover Active Directory sites and subnets, and then create Configuration Manager boundaries based on those network locations.
- Identify supernets that are assigned to an Active Directory site. Convert each supernet into an IP address range boundary.
- Publish to Active Directory Domain Services (AD DS) in a forest when publishing to that forest is enabled. The specified Active Directory Forest Account must have permissions to that forest.

You can manage Active Directory Forest Discovery in the Configuration Manager console. Go to the **Administration** workspace and expand **Hierarchy Configuration**.

- **Discovery Methods**: Enable Active Directory Forest Discovery to run at the top-level site of your hierarchy. You can also specify a simple schedule to run discovery. Configure it to automatically create boundaries from the IP subnets and Active Directory sites that it discovers. Active Directory Forest Discovery cannot be run at a child primary site or at a secondary site.
- **Active Directory Forests**: Configure the additional forests to discover, specify each Active Directory Forest Account, and configure publishing to each forest. Monitor the discovery process. Add IP subnets and Active Directory sites as Configuration Manager boundaries and members of boundary groups.

To configure publishing for Active Directory forests for each site in your hierarchy, connect your Configuration Manager console to the top-level site of your hierarchy. The **Publishing** tab in an Active Directory site's

Properties dialog box can show only the current site and its child sites. When publishing is enabled for a forest, and that forest's schema is extended for Configuration Manager, the following information is published for each site that is enabled to publish to that Active Directory forest:

- **SMS-Site-<site code>**
- **SMS-MP-<site code>-<site system server name>**
- **SMS-SLP-<site code>-<site system server name>**
- **SMS-<site code>-<Active Directory site name or subnet>**

> **NOTE**
> Secondary sites always use the secondary site server computer account to publish to Active Directory. If you want secondary sites to publish to Active Directory, ensure that the secondary site server computer account has permissions to publish to Active Directory. A secondary site cannot publish data to an untrusted forest.

Caution

When you uncheck the option to publish a site to an Active Directory forest, all previously published information for that site, including available site system roles, is removed from Active Directory.

Actions for Active Directory Forest Discovery are recorded in the following logs:

- All actions, except actions related to publishing, are recorded in the **ADForestDisc.Log** file in the **<InstallationPath>\Logs** folder on the site server.
- Active Directory Forest Discovery publishing actions are recorded in the **hman.log** and **sitecomp.log** files in the **<InstallationPath>\Logs** folder on the site server.

For more information about how to configure this discovery method, see Configure discovery methods.

Active Directory Group Discovery

Configurable: Yes

Enabled by default: No

Accounts you can use to run this method:

- **Active Directory Group Discovery Account** (user defined)
- **Computer account** of the site server

> **TIP**
> In addition to the information in this section, see Common features of Active Directory Group, System, and User Discovery.

Use this method to search Active Directory Domain Services to identify:

- Local, global, and universal security groups.
- The membership of groups.
- Limited information about a group's member computers and users, even when another discovery method has not previously discovered those computers and users.

This discovery method is intended to identify groups and the group relationships of members of groups. By default, only security groups are discovered. If you want to also find the membership of distribution groups, you

must check the box for the option **Discover the membership of distribution groups** on the **Option** tab in the **Active Directory Group Discovery Properties** dialog box.

Active Directory Group Discovery doesn't support the extended Active Directory attributes that can be identified by using Active Directory System Discovery or Active Directory User Discovery. Because this discovery method isn't optimized to discover computer and user resources, consider running this discovery method after you have run Active Directory System Discovery and Active Directory User Discovery. This suggestion is because this method creates a full discovery data record (DDR) for groups, but only a limited DDR for computers and users that are members of groups.

You can configure the following discovery scopes that control how this method searches for information:

- **Location**: Use a location if you want to search one or more Active Directory containers. This scope option supports a recursive search of the specified Active Directory containers. This process searches each child container under the container that you specify. It continues until no more child containers are found.
- **Groups**: Use groups if you want to search one or more specific Active Directory groups. You can configure **Active Directory Domain** to use the default domain and forest, or limit the search to an individual domain controller. Additionally, you can specify one or more groups to search. If you do not specify at least one group, all groups found in the specified **Active Directory Domain** location are searched.

Caution

When you configure a discovery scope, choose only the groups that you must discover. This recommendation is because Active Directory Group Discovery tries to discover each member of each group in the discovery scope. Discovery of large groups can require extensive use of bandwidth and Active Directory resources.

> **NOTE**
>
> Before you can create collections that are based on extended Active Directory attributes, and to ensure accurate discovery results for computers and users, run Active Directory System Discovery or Active Directory User Discovery, depending on what you want to discover.

Actions for Active Directory Group Discovery are recorded in the file **adsgdis.log** in the **<InstallationPath>\LOGS** folder on the site server.

For more information about how to configure this discovery method, see Configure discovery methods.

Active Directory System Discovery

Configurable: Yes

Enabled by default: No

Accounts you can use to run this method:

- **Active Directory System Discovery Account** (user defined)
- **Computer account** of the site server

> **TIP**
>
> In addition to the information in this section, see Common features of Active Directory Group, System, and User Discovery.

Use this discovery method to search the specified Active Directory Domain Services locations for computer resources that can be used to create collections and queries. You can also install the Configuration Manager client on a discovered device by using client push installation.

By default, this method discovers basic information about the computer, including the following attributes:

- Computer name
- Operating system and version
- Active Directory container name
- IP address
- Active Directory site
- Time stamp of last logon

To successfully create a DDR for a computer, Active Directory System Discovery must be able to identify the computer account and then successfully resolve the computer name to an IP address.

In the **Active Directory System Discovery Properties** dialog box, on the **Active Directory Attributes** tab, you can view the full list of default object attributes that it discovers. You can also configure the method to discover additional (extended) attributes.

Actions for Active Directory System Discovery are recorded in the file **adsysdis.log** in the **<InstallationPath>\LOGS** folder on the site server.

For more information about how to configure this discovery method, see Configure discovery methods.

Active Directory User Discovery

Configurable: Yes

Enabled by default: No

Accounts you can use to run this method:

- **Active Directory User Discovery Account** (user defined)
- **Computer account** of the site server

> **TIP**
> In addition to the information in this section, see Common features of Active Directory Group, System, and User Discovery.

Use this discovery method to search Active Directory Domain Services to identify user accounts and associated attributes. By default, this method discovers basic information about the user account, including the following attributes:

- User name
- Unique user name (includes domain name)
- Domain
- Active Directory container names

In the **Active Directory User Discovery Properties** dialog box, on the **Active Directory Attributes** tab, you can view the full default list of object attributes that it discovers. You can also configure the method to discover additional (extended) attributes.

Actions for Active Directory User Discovery are recorded in the file **adusrdis.log** in the **<InstallationPath>\LOGS** folder on the site server.

For more information about how to configure this discovery method, see Configure discovery methods.

Azure Active Directory User Discovery

Use Azure Active Directory (Azure AD) User Discovery to search your Azure AD subscription for users with a modern cloud identity. Azure AD user discovery can find the following attributes:

- objectId
- displayName
- mail
- mailNickname
- onPremisesSecurityIdentifier
- userPrincipalName
- AAD tenantID
- onPremisesDomainName
- onPremisesSamAccountName
- onPremisesDistinguishedName

This method supports full and delta synchronization of user attributes from Azure AD. This information can then be used along-side discovery data you collect from the other discovery methods.

Actions for Azure AD user discovery are recorded in the **SMS_AZUREAD_DISCOVERY_AGENT.log** file on the top-tier site server of the hierarchy.

To configure Azure AD user discovery, see Configure Azure Services for Cloud Management. For information about how to configure this discovery method, see Configure Azure AD User Discovery.

Azure Active Directory user group discovery

(Introduced as a pre-release feature in version 1906)

You can discover user groups and members of those groups from Azure Active directory (Azure AD). Azure AD user group discovery can find the following attributes:

- objectId
- displayName
- mailNickname
- onPremisesSecurityIdentifier
- AAD tenantID

Actions for Azure AD user group discovery are recorded in the **SMS_AZUREAD_DISCOVERY_AGENT.log** file on the top-tier site server of the hierarchy. For information about how to configure this discovery method, see Configure Azure AD user group discovery.

Heartbeat Discovery

Configurable: Yes

Enabled by default: Yes

Accounts you can use to run this method:

- **Computer account** of the site server

Heartbeat Discovery differs from other Configuration Manager discovery methods. It is enabled by default and runs on each computer client (instead of on a site server) to create a DDR. For mobile device clients, this DDR is

created by the management point that the mobile device client is using. To help maintain the database record of Configuration Manager clients, do not disable Heartbeat Discovery. In addition to maintaining the database record, this method can force discovery of a computer as a new resource record. It can also repopulate the database record of a computer that was deleted from the database.

Heartbeat Discovery runs on a schedule configured for all clients in the hierarchy. The default schedule for Heartbeat Discovery is set to every seven days. If you change the heartbeat discovery interval, ensure that it runs more frequently than the site maintenance task **Delete Aged Discovery Data**. This task deletes inactive client records from the site database. You can configure the **Delete Aged Discovery Data** task only for primary sites.

You can also manually invoke Heartbeat Discovery on a specific client. Run the **Discovery Data Collection Cycle** on the **Action** tab of a client's Configuration Manager control panel.

When Heartbeat Discovery runs, it creates a DDR that has the client's current information. The client then copies this small file (about 1 KB in size) to a management point so that a primary site can process it. The file has the following information:

- Network location
- NetBIOS name
- Version of the client agent
- Operational status details

Heartbeat Discovery is the only discovery method that provides details about the client installation status. It does so by updating the system resource client attribute to set a value equal to **Yes**.

> **NOTE**
> Even when Heartbeat Discovery is disabled, DDRs are still created and submitted for active mobile device clients. This behavior ensures that the task to **Delete Aged Discovery Data** doesn't affect active mobile devices. When the **Delete Aged Discovery Data** task deletes a database record for a mobile device, it also revokes the device certificate. This action blocks the mobile device from connecting to management points.

Actions for Heartbeat Discovery are logged in the following locations:

- For computer clients, Heartbeat Discovery actions are recorded on the client in the **InventoryAgent.log** file in the *%Windir%\CCM\Logs* folder.
- For mobile device clients, Heartbeat Discovery actions are recorded in the **DMPRP.log** file in the *%Program Files%\CCM\Logs* folder of the management point that the mobile device client uses.

For more information about how to configure this discovery method, see Configure discovery methods.

Network Discovery

Configurable: Yes

Enabled by default: No

Accounts you can use to run this method:

- **Computer account** of the site server

Use this method to discover the topology of your network and to discover devices on your network that have an IP address. Network Discovery searches your network for IP-enabled resources by querying the following entities:

- Servers that run a Microsoft implementation of DHCP

- Address Resolution Protocol (ARP) caches in network routers
- SNMP-enabled devices
- Active Directory domains

Before you can use Network Discovery, you must specify the *level* of discovery to run. You also configure one or more discovery mechanisms that enable Network Discovery to query for network segments or devices. You can also configure settings that help control discovery actions on the network. Finally, you define one or more schedules for when Network Discovery runs.

For this method to successfully discover a resource, Network Discovery must identify the IP address and the subnet mask of the resource. The following methods are used to identify the subnet mask of an object:

- **Router ARP cache:** Network Discovery queries the ARP cache of a router to find subnet information. Typically, data in a router ARP cache has a short time-to-live. Therefore, when Network Discovery queries the ARP cache, the ARP cache might no longer have information about the requested object.
- **DHCP:** Network Discovery queries each DHCP server that you specify to discover the devices for which the DHCP server has provided a lease. Network Discovery supports only DHCP servers that run the Microsoft implementation of DHCP.
- **SNMP device:** Network Discovery can directly query an SNMP device. For Network Discovery to query a device, the device must have a local SNMP agent installed. Also configure Network Discovery to use the community name that the SNMP agent is using.

When discovery identifies an IP-addressable object and can determine the object's subnet mask, it creates a DDR for that object. Because different types of devices connect to the network, Network Discovery discovers resources that don't support the Configuration Manager client. For example, devices that can be discovered but not managed include printers and routers.

Network Discovery can return several attributes as part of the discovery record that it creates. These attributes include:

- NetBIOS name
- IP addresses
- Resource domain
- System roles
- SNMP community name
- MAC addresses

Network Discovery activity is recorded in the **Netdisc.log** file in *<InstallationPath>\Logs* on the site server that runs discovery.

For more information about how to configure this discovery method, see Configure discovery methods.

> **NOTE**
>
> Complex networks and low-bandwidth connections can cause Network Discovery to run slowly and generate significant network traffic. As a best practice, run Network Discovery only when the other discovery methods cannot find the resources that you have to discover. For example, use Network Discovery if you must discover workgroup computers. Other discovery methods do not discover workgroup computers.

Levels of Network Discovery

When you configure Network Discovery, you specify one of three levels of discovery:

LEVEL OF DISCOVERY	DETAILS
Topology	This level discovers routers and subnets but does not identify a subnet mask for objects.
Topology and client	In addition to topology, this level discovers potential clients like computers, and resources like printers and routers. This level of discovery tries to identify the subnet mask of objects that it finds.
Topology, client, and client operating system	In addition to topology and potential clients, this level tries to discover the computer operating system name and version. This level uses Windows Browser and Windows Networking calls.

With each incremental level, Network Discovery increases its activity and network bandwidth usage. Consider the network traffic that can be generated before you enable all aspects of Network Discovery.

For example, when you first use Network Discovery, you might start with only the topology level to identify your network infrastructure. Then, reconfigure Network Discovery to discover objects and their device operating systems. You can also configure settings that limit Network Discovery to a specific range of network segments. That way, you discover objects in network locations that you require and avoid unnecessary network traffic. This process also allows you to discover objects from edge routers or from outside your network.

Network Discovery options

To enable Network Discovery to search for IP-addressable devices, configure one or more of these options.

> **NOTE**
> Network Discovery runs in the context of the computer account of the site server that runs discovery. If the computer account does not have permissions to an untrusted domain, the domain and DHCP server configurations can fail to discover resources.

DHCP

Specify each DHCP server that you want Network Discovery to query. (Network Discovery supports only DHCP servers that run the Microsoft implementation of DHCP.)

- Network Discovery retrieves information by using remote procedure calls to the database on the DHCP server.
- Network Discovery can query both 32-bit and 64-bit DHCP servers for a list of devices that are registered with each server.
- For Network Discovery to successfully query a DHCP server, the computer account of the server that runs discovery must be a member of the DHCP Users group on the DHCP server. For example, this level of access exists when one of the following statements is true:
  - The specified DHCP server is the DHCP server of the server that runs discovery.
  - The computer that runs discovery and the DHCP server are in the same domain.
  - A two-way trust exists between the computer that runs discovery and the DHCP server.
  - The site server is a member of the DHCP Users group.
- When Network Discovery enumerates a DHCP server, it does not always discover static IP addresses. Network Discovery does not find IP addresses that are part of an excluded range of IP addresses on the DHCP server. It also does not discover IP addresses that are reserved for manual assignment.

Domains

Specify each domain that you want Network Discovery to query.

- The computer account of the site server that runs discovery must have permissions to read the domain controllers in each specified domain.
- To discover computers from the local domain, you must enable the Computer Browser service on at least one computer. This computer must be on the same subnet as the site server that runs Network Discovery.
- Network Discovery can discover any computer that you can view from your site server when you browse the network.
- Network Discovery retrieves the IP address. It then uses an Internet Control Message Protocol (ICMP) echo request to ping each device that it finds. The **ping** command helps determine which computers are currently active.

SNMP Devices

Specify each SNMP device that you want Network Discovery to query.

- Network Discovery retrieves the ipNetToMediaTable value from any SNMP device that responds to the query. This value returns arrays of IP addresses that are client computers or other resources like printers, routers, or other IP-addressable devices.
- To query a device, you must specify the IP address or NetBIOS name of the device.
- Configure Network Discovery to use the community name of the device, or the device rejects the SNMP-based query.

Limiting Network Discovery

When Network Discovery queries an SNMP device on the edge of your network, it can identify information about subnets and SNMP devices that are outside your immediate network. Use the following information to limit Network Discovery by configuring the SNMP devices that discovery can communicate with, and by specifying the network segments to query.

Subnets

Configure the subnets that Network Discovery queries when it uses the SNMP and DHCP options. These two options search only the enabled subnets.

For example, a DHCP request can return devices from locations across your whole network. If you want to discover only devices on a specific subnet, specify and enable that specific subnet on the **Subnets** tab in the **Network Discovery Properties** dialog box. When you specify and enable subnets, you limit future DHCP and SNMP discovery tasks to those subnets.

> **NOTE**
>
> Subnet configurations do not limit the objects that the **Domains** discovery option discovers.

SNMP community names

To enable Network Discovery to successfully query an SNMP device, configure Network Discovery with the community name of the device. If Network Discovery is not configured by using the community name of the SNMP device, the device rejects the query.

Maximum hops

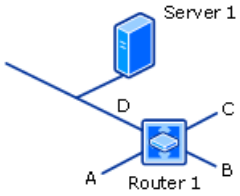
When you configure the maximum number of router hops, you limit the number of network segments and routers that Network Discovery can query by using SNMP.

The number of hops that you configure limits the number of additional devices and network segments that

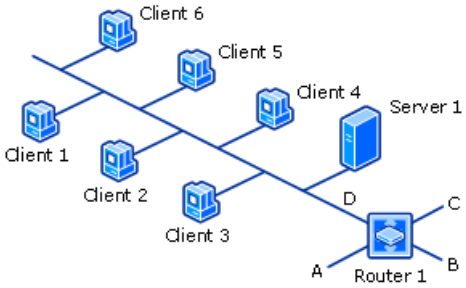
Network Discovery can query.

For example, a topology-only discovery with **0** (zero) router hops discovers the subnet on which the originating server resides. It includes any routers on that subnet.

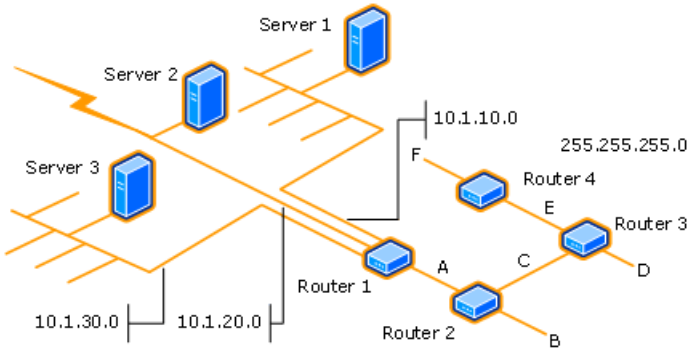
The following diagram shows what a topology-only Network Discovery query finds when it runs on Server 1 with 0 router hops specified: subnet D and Router 1.



The following diagram shows what a topology and client Network Discovery query finds when it runs on Server 1 with 0 router hops specified: subnet D and Router 1, and all potential clients on subnet D.



To get a better idea of how additional router hops can increase the amount of network resources that are discovered, consider the following network:



Running a topology-only Network Discovery from Server 1 with one router hop discovers the following entities:

- Router 1 and subnet 10.1.10.0 (found with zero hops)
- Subnets 10.1.20.0 and 10.1.30.0, subnet A, and Router 2 (found on the first hop)

> **WARNING**
> Each increase to the number of router hops can significantly increase the number of discoverable resources and increase the network bandwidth that Network Discovery uses.

Server Discovery

Configurable: No

In addition to the user-configurable discovery methods, Configuration Manager uses a process named **Server Discovery** (SMS_WINNT_SERVER_DISCOVERY_AGENT). This discovery method creates resource records for computers that are site systems, like a computer that is configured as a management point.

Common features of Active Directory Group Discovery, System Discovery, and User Discovery

This section provides information about features that are common to the following discovery methods:

- Active Directory Group Discovery
- Active Directory System Discovery
- Active Directory User Discovery

> **NOTE**
> The information in this section does not apply to Active Directory Forest Discovery.

These three discovery methods are similar in configuration and operation. They can discover computers, users, and information about group memberships of resources that are stored in Active Directory Domain Services. The discovery process is managed by a discovery agent. The agent runs on the site server at each site where discovery is configured to run. You can configure each of these discovery methods to search one or more Active Directory locations as location instances in the local forest or remote forests.

When discovery searches an untrusted forest for resources, the discovery agent must be able to resolve the following to be successful:

- To discover a computer resource by using Active Directory System Discovery, the discovery agent must be able to resolve the FQDN of the resource. If it cannot resolve the FQDN, it then tries to resolve the resource by its NetBIOS name.
- To discover a user or group resource by using Active Directory User Discovery or Active Directory Group Discovery, the discovery agent must be able to resolve the FQDN of the domain controller name that you specify for the Active Directory location.

For each location that you specify, you can configure individual search options, like enabling a recursive search of the location's Active Directory child containers. You can also configure a unique account to use when it searches that location. This account provides flexibility in configuring a discovery method at one site to search multiple Active Directory locations across multiple forests. You don't have to configure a single account that has permissions to all locations.

When each of these three discovery methods runs at a specific site, the Configuration Manager site server at that site contacts the nearest domain controller in the specified Active Directory forest to locate Active Directory resources. The domain and forest can be in any supported Active Directory mode. The account that you assign to each location instance must have **Read** access permission to the specified Active Directory locations.

Discovery searches the specified locations for objects and then tries to collect information about those objects. A DDR is created when sufficient information about a resource can be identified. The required information varies depending on the discovery method that is being used.

If you configure the same discovery method to run at different Configuration Manager sites to take advantage of querying local Active Directory servers, you can configure each site with a unique set of discovery options. Because discovery data is shared with each site in the hierarchy, avoid overlap between these configurations to efficiently discover each resource a single time.

For smaller environments, consider running each discovery method at only one site in your hierarchy. This configuration reduces administrative overhead and the potential for multiple discovery actions to rediscover the same resources. When you minimize the number of sites that run discovery, you reduce the overall network bandwidth that discovery uses. You can also reduce the overall number of DDRs that are created and must be

processed by your site servers.

Many of the discovery method configurations are self-explanatory. Use the following sections for more information about the discovery options that might require additional information before you configure them.

The following options are available for use with multiple Active Directory discovery methods:

- Delta Discovery
- Filter stale computer records by domain logon
- Filter stale records by computer password
- Search customized Active Directory attributes

Delta Discovery

Available for:

- Active Directory Group Discovery
- Active Directory System Discovery
- Active Directory User Discovery

Delta Discovery is not an independent discovery method but an option available for the applicable discovery methods. Delta Discovery searches specific Active Directory attributes for changes that were made since the last full discovery cycle of the applicable discovery method. The attribute changes are submitted to the Configuration Manager database to update the discovery record of the resource.

By default, Delta Discovery runs on a five-minute cycle. This schedule is much more frequent than the typical schedule for a full discovery cycle. This frequent cycle is possible because Delta Discovery uses fewer site server and network resources than a full discovery cycle does. When you use Delta Discovery, you can reduce the frequency of the full discovery cycle for that discovery method.

The following are the most common changes that Delta Discovery detects:

- New computers or users added to Active Directory
- Changes to basic computer and user information
- New computers or users that are added to a group
- Computers or users that are removed from a group
- Changes to system group objects

Although Delta Discovery can detect new resources and changes to group membership, it cannot detect when a resource has been deleted from Active Directory. DDRs created by Delta Discovery are processed similarly to the DDRs that are created by a full discovery cycle.

You configure Delta Discovery on the **Polling Schedule** tab in the properties for each discovery method.

Filter stale computer records by domain logon

Available for:

- Active Directory Group Discovery
- Active Directory System Discovery

You can configure discovery to exclude computers with a stale computer record. This exclusion is based on the last domain logon of the computer. When this option is enabled, Active Directory System Discovery evaluates each computer that it identifies. Active Directory Group Discovery evaluates each computer that is a member of a group

that is discovered.

To use this option:

- Computers must be configured to update the **lastLogonTimeStamp** attribute in Active Directory Domain Services.
- The Active Directory domain functional level must be set to Windows Server 2003 or later.

When you're configuring the time after the last logon that you want to use for this setting, consider the interval for replication between domain controllers.

You configure filtering on the **Option** tab in the **Active Directory System Discovery Properties** and **Active Directory Group Discovery Properties** dialog boxes. Choose to **Only discover computers that have logged on to a domain in a given period of time**.

> **WARNING**
> When you configure this filter and **Filter stale records by computer password**, discovery excludes computers that meet the criteria of either filter.

Filter stale records by computer password

Available for:

- Active Directory Group Discovery
- Active Directory System Discovery

You can configure discovery to exclude computers with a stale computer record. This exclusion is based on the last computer account password update by the computer. When this option is enabled, Active Directory System Discovery evaluates each computer that it identifies. Active Directory Group Discovery evaluates each computer that is a member of a group that is discovered.

To use this option:

- Computers must be configured to update the **pwdLastSet** attribute in Active Directory Domain Services.

When you're configuring this option, consider the interval for updates to this attribute. Also consider the replication interval between domain controllers.

You configure filtering on the **Option** tab in the **Active Directory System Discovery Properties** and **Active Directory Group Discovery Properties** dialog boxes. Choose to **Only discover computers that have updated their computer account password in a given period of time**.

> **WARNING**
> When you configure this filter and **Filter stale records by domain logon**, discovery excludes computers that meet the criteria of either filter.

Search customized Active Directory attributes

Available for:

- Active Directory System Discovery
- Active Directory User Discovery

Each discovery method supports a unique list of Active Directory attributes that can be discovered.

You can view and configure the list of customized attributes on the **Active Directory Attributes** tab in the **Active Directory System Discovery Properties** and **Active Directory User Discovery Properties** dialog boxes.

Select discovery methods to use for System Center Configuration Manager

5/9/2019 • 9 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To successfully and efficiently use discovery for System Center Configuration Manager, you must consider which methods to use and at which sites to run them.

Because discovery can generate a large volume of network traffic, and the resultant discovery data records (DDRs) can use significant CPU resources during processing, use only those discovery methods that you require to meet your goals. You might start by using only one or two discovery methods, and then later enable additional methods in a controlled manner to extend the level of discovery in your environment. The information in this topic can help you make informed decisions.

For information about the different discovery methods, see About discovery methods for System Center Configuration Manager.

Select methods to discover different things

To discover potential Configuration Manager client computers or user resources, you must enable the appropriate discovery methods. You can use different combinations of discovery methods to locate different resources, and to discover additional information about those resources. The discovery methods that you use determine the type of resources that are discovered, and which Configuration Manager services and agents are used in the discovery process. They also determine the type of information about resources that you can discover.

Discover computers

When you want to discover computers, you can use **Active Directory System Discovery** or **Network Discovery**.

For example, if you want to discover resources that can install the Configuration Manager client before you use client push installation, you might run Active Directory System Discovery. Using this method, you not only discover the resource, but also discover basic information even extended information about it from Active Directory Domain Services. This information might be useful in building complex queries and collections to use for the assignment of client settings or content deployment.

Alternatively, you could run Network Discovery, and use its options to discover the operating system of resources (required to later use client push installation). Network Discovery provides you with information about your network topology that you are not able to acquire with other discovery methods. This method does not, however, provide you any information about your Active Directory environment.

There is also a method called **Heartbeat Discovery**. It is possible to use only Heartbeat Discovery to force the discovery of clients that you installed by methods other than client push installation. However, unlike other discovery methods, Heartbeat Discovery cannot discover computers that do not have an active Configuration Manager client. It returns a limited set of information, intended to maintain an existing database record rather than be the basis of that record. Information submitted by Heartbeat Discovery might not be sufficient to build complex queries or collections.

If you use **Active Directory Group Discovery** to discover the membership of a specified group, you can discover limited system or computer information. This does not replace a full discovery of computers, but can provide basic information. This information is insufficient for client push installation.

Discover users

When you want to discover information about users, use **Active Directory User Discovery**. Similar to Active Directory System Discovery, this method discovers users from Active Directory. It includes basic information, in addition to extended Active Directory information. You can use this information to build complex queries and collections similar to those for computers.

Discover group information

When you want to discover information about groups and group memberships, use **Active Directory Group Discovery**. This discovery method creates resource records for security groups.

You can use this method to search a specific Active Directory group to identify the members of that group, in addition to any nested groups within that group. You can also use this method to search an Active Directory location for groups, and recursively search each child container of that location in Active Directory Domain Services.

This discovery method can also search the membership of distribution groups. This can identify the group relationships of both users and computers.

When you discover a group, you can also discover limited information about its members. This does not replace the Active Directory system or user discovery methods, though. It is usually insufficient to build complex queries and collections, or serve as the basis of a client push installation.

Discover infrastructure

There are two methods you can use to discover network infrastructure, **Active Directory Forest Discovery** and **Network Discovery**.

Use Active Directory Forest Discovery to search an Active Directory forest for information about subnets and Active Directory site configurations. These configurations can then be automatically entered into Configuration Manager as boundary locations.

When you want to discover your network topology, use Network Discovery. While other discovery methods return information related to Active Directory Domain Services, and can identify the current network location of a client, they do not provide infrastructure information based on the subnets and router topology of your network.

Discovery data is shared among sites

After Configuration Manager adds discovery data to a database, it is quickly shared among all sites in the hierarchy. Because there is typically no benefit to discovering the same information at multiple sites in your hierarchy, consider setting up a single instance of each discovery method that you use to run at a single site. It's a good idea to do this instead of running multiple instances of a single method at different sites.

However, for some environments it might be useful to assign the same discovery method to run at multiple sites, each with a separate configuration and schedule. For example, when using Network Discovery, you might want to direct each site to discover its local network, instead of attempting to discover all network locations across a WAN.

If you do configure multiple instances of the same discovery methods to run at different sites, plan the configuration of each site carefully. You want to avoid having two or more sites discover the same resources from your network or Active Directory. This can consume additional network bandwidth and create duplicate DDRs.

The following table identifies at which sites you can set up the different discovery methods.

DISCOVERY METHOD	SUPPORTED LOCATIONS
Active Directory Forest Discovery	Central administration site Primary site

DISCOVERY METHOD	SUPPORTED LOCATIONS
Active Directory Group Discovery	Primary site
Active Directory System Discovery	Primary site
Active Directory User Discovery	Primary site
Heartbeat Discovery[1]	Primary site
Network Discovery	Primary site Secondary site

[1] Secondary sites cannot configure Heartbeat Discovery, but can receive the Heartbeat DDR from a client.

When secondary sites run Network Discovery, or receive Heartbeat Discovery DDRs, they transfer the DDR by file-based replication to their parent primary site. This is because only primary sites and central administration sites can process DDRs. For more information about how DDRs are processed, see About discovery data records.

Considerations for different discovery methods

Because each site server and network environment is different, it's a good idea to limit your initial configurations for discovery. Then closely monitor each site server for its ability to process the discovery data that is generated.

When you use an **Active Directory** discovery method for systems, users, or groups:

- Run discovery at a site that has a fast network connection to your domain controllers.
- Consider the Active Directory replication topology to ensure discovery can access the latest information.
- Consider the scope of the discovery configuration, and limit discovery to only those Active Directory locations and groups that you have to discover.

If you use **Network Discovery**:

- Use a limited initial configuration to identify your network topography.
- After you identify your network topography, set up Network Discovery to run at specific sites that are central to the network areas that you want to more fully discover.

Because **Heartbeat Discovery** does not run at a specific site, you do not have to consider it in general planning for where to run discovery.

Best practices for discovery

For best results with discovery, we recommend the following:

- **Run Active Directory System Discovery and Active Directory User Discovery before you run Active Directory Group Discovery.**

  When Active Directory Group Discovery identifies a previously undiscovered user or computer as a member of a group, it attempts to discover basic details for the user or computer. Because Active Directory Group Discovery is not optimized for this type of discovery, this process can cause it to run slowly. Additionally, Active Directory Group Discovery identifies only the basic details about the users and computers it discovers, and does not create a complete user or computer discovery record. When you run Active Directory System Discovery and Active Directory User Discovery, the additional Active Directory

attributes for each object type are available. As a result, Active Directory Group Discovery runs more efficiently.

- **When you set up Active Directory Group Discovery, only specify groups that you use with Configuration Manager.**

  To help control the use of resources by Active Directory Group Discovery, specify only those groups that you use with Configuration Manager. This is because Active Directory Group Discovery recursively searches each group it discovers for users, computers, and nested groups. The search of each nested group can expand the scope of Active Directory Group Discovery, and reduce performance. Additionally, when you set up delta discovery for Active Directory Group Discovery, the discovery method monitors each group for changes. This further reduces performance when the method must search unnecessary groups.

- **Set up discovery methods with a longer interval between full discovery, and a more frequent period of delta discovery.**

  Because delta discovery uses fewer resources than a full discovery cycle, and can identify new or modified resources in Active Directory, you can reduce the frequency of full discovery cycles to run weekly (or less). Delta discovery for Active Directory System Discovery, Active Directory User Discovery and Active Directory Group Discovery identifies almost all the changes of Active Directory objects, and can maintain accurate discovery data for resources.

- **Run Active Directory discovery methods at a primary site that has a network location that is closest to your Active Directory domain controller.**

  To improve the performance of Active Directory discovery, it's a good idea to run discover at a primary site that has a fast network connection to your domain controllers. If you run the same Active Directory discovery method at multiple sites, set up each discovery method to avoid overlap. Unlike past versions of Configuration Manager, discovery data is shared among sites. Therefore, it is not necessary to discover the same information at multiple sites. For more information, see Discovery data is shared between sites.

- **Run Active Directory Forest Discovery at only one site when you plan to automatically create boundaries from the discovery data.**

  If you run Active Directory Forest Discovery at more than one site in a hierarchy, it's a good idea to only enable options to automatically create boundaries at a single site. This is because when Active Directory Forest Discovery runs at each site and creates boundaries, Configuration Manager cannot merge those boundaries into a single boundary object. When you configure Active Directory Forest Discovery to automatically create boundaries at multiple sites, the result can be duplicated boundary objects in the Configuration Manager console.

Configure discovery methods for Configuration Manager

8/1/2019 • 22 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configure discovery methods to find resources to manage from your network, Active Directory, and Azure Active Directory (Azure AD). First enable and then configure each method that you want to use to search your environment. You can also disable a method by using the same procedure that you use to enable it. The only exceptions to this process are Heartbeat Discovery and Server Discovery:

- By default, **Heartbeat Discovery** is already enabled when you install a Configuration Manager primary site. It's configured to run on a basic schedule. Keep Heartbeat Discovery enabled. It makes sure that the discovery data records (DDRs) for devices are up-to-date. For more information about Heartbeat Discovery, see About Heartbeat Discovery.
- **Server Discovery** is an automatic discovery method. It finds computers that you use as site systems. You can't configure or disable it.

Active Directory Forest Discovery

To finish the configuration of Active Directory Forest Discovery, configure settings in the following locations of the Configuration Manager console:

- In the **Discovery Methods** node:
  - Enable this discovery method.
  - Set a polling schedule.
  - Select whether discovery automatically creates boundaries for the Active Directory sites and subnets that it discovers.
- In the **Active Directory Forests** node:
  - Add forests that you want to discover.
  - Enable discovery of Active Directory sites and subnets in that forest.
  - Configure settings that enable Configuration Manager sites to publish their site information to the forest.
  - Assign an account to use as the Active Directory Forest Account for each forest.

Use the following procedures to enable Active Directory Forest Discovery, and to configure individual forests for use with Active Directory Forest Discovery.

Configure Active Directory Forest Discovery

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Hierarchy Configuration**, and select the **Discovery Methods** node.
2. Select the Active Directory Forest Discovery method for the site where you want to configure discovery.
3. On the **Home** tab of the ribbon, select **Properties**.

4. On the **General** tab of the properties, configure the following settings:
   - Enable the discovery method.
   - Specify options to create site boundaries for discovered locations.
   - Specify a schedule for when discovery runs.
5. Select **OK** to save the configuration.

Configure a forest for Active Directory Forest Discovery

1. In the **Administration** workspace, expand **Hierarchy Configuration**, and select the **Active Directory Forests** node. If Active Directory Forest Discovery has previously run, you see each discovered forest in the results pane. When this discovery method runs, it discovers the local forest and any trusted forests. Manually add untrusted forests.
   - To configure a previously discovered forest, select the forest in the results pane. In the ribbon, select **Properties** to open the forest properties.
   - To configure a new forest that isn't listed, on the **Home** tab of the ribbon, in the **Create** group, select **Add Forest**. This action opens the **Add Forests** dialog box.
2. On the **General** tab, finish configurations for the forest that you want to discover, and specify the **Active Directory Forest Account**. For more information on this account, see Accounts.

   > **NOTE**
   > Active Directory Forest Discovery requires a global account to discover and publish to untrusted forests. If you don't use the computer account of the site server, you can only select a global account.

3. If you plan to let sites publish site data to this forest, on the **Publishing** tab, finish configurations for publishing to this forest.

   > **NOTE**
   > If you let sites publish to a forest, extend the Active Directory schema of that forest for Configuration Manager. The Active Directory Forest Account must have Full Control permissions to the System container in that forest.

4. Select **OK** to save the configuration.

Active Directory discovery for computers, users, or groups

To configure discovery of computers, users, or groups, start with these common steps:

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Hierarchy Configuration**, and select the **Discovery Methods** node.
2. Select the method for the site where you want to configure discovery.
3. On the **Home** tab of the ribbon, select **Properties**.
4. On the **General** tab of the properties, select the checkbox to enable discovery. Or you can configure discovery now, and then return to enable discovery later.

Then use the information in the following sections to configure the specific discovery methods:

- Active Directory Group Discovery

- Active Directory System Discovery
- Active Directory User Discovery

> **NOTE**
> The information in this section doesn't apply to Active Directory Forest Discovery.

Although each of these discovery methods is independent of the others, they share similar options. For more information about these configuration options, see Shared options for group, system, and user discovery.

> **WARNING**
> The Active Directory polling by each of these discovery methods can generate significant network traffic. Consider scheduling each discovery method to run at a time when this network traffic doesn't adversely affect business uses of your network.

Configure Active Directory Group Discovery

1. On the **General** tab of the Active Directory Group Discovery Properties window, select **Add** to configure a discovery scope. Select either **Groups** or **Location**. Then finish the following configurations in the **Add Groups** or **Add Active Directory Location** dialog box:
   a. Specify a **Name** for this discovery scope.
   b. Specify an **Active Directory Domain** or **Location** to search:
      - If you chose **Groups**, specify one or more Active Directory groups to discover.
      - If you chose **Location**, specify an Active Directory container as a location to discover. You can also enable a recursive search of Active Directory child containers for this location.
   c. Specify the **Active Directory Group Discovery Account** that the site uses to search this discovery scope. For more information, see Accounts.
   d. Select **OK** to save the discovery scope configuration.
2. Repeat the previous steps for each additional discovery scope that you want to define.
3. On the **Polling Schedule** tab, configure both the full discovery polling schedule and delta discovery.
4. On the **Options** tab, configure settings to filter out or exclude stale computer records from discovery. Also configure the discovery of the membership of distribution groups.

   > **NOTE**
   > By default, Active Directory Group Discovery discovers only the membership of security groups.

5. Select **OK** to save the configuration.

Configure Active Directory System Discovery

1. On the **General** tab of the Active Directory System Discovery Properties window, select the **New** icon to specify a new Active Directory container. In the **Active Directory Container** dialog box, finish the following configurations:
   a. Type or browse to a location for the **Path**. This value is a valid LDAP path to a container or organizational unit (OU). The site queries this path for resources. For example, `LDAP://CN=Computers,DC=contoso,DC=com`

b. Specify options that change the search behavior:

- **Discover objects within Active Directory groups**: The site also looks at the membership of groups in this path.
- **Recursively search Active Directory child containers**: If you enable this option, the site searches any additional containers or OUs within the above path. If you disable this option, the site only searches for resources in the specific path.

  Starting in version 1806, select subcontainers to exclude from this recursive search. This option helps to reduce the number of discovered objects. Select **Add** to choose the containers under the above path. In the Select New Container dialog box, select a child container to exclude. Select **OK** to close the Select New Container dialog box.

  > **TIP**
  > The list of Active Directory containers in the Active Directory System Discovery Properties window includes a column **Has Exclusions**. When you select containers to exclude, this value is **Yes**.

c. For each location, specify the account to use as the **Active Directory Discovery Account**. For more information, see Accounts.

> **TIP**
> For each specified location, you can configure a set of discovery options and a unique Active Directory Discovery Account.

d. Select **OK** to save the Active Directory container configuration.

2. On the **Polling Schedule** tab, configure both the full discovery polling schedule and delta discovery.
3. On the **Active Directory Attributes** tab, configure additional Active Directory attributes for computers that you want to discover. This tab lists the default object attributes.

> **TIP**
> For example, your organization uses the **Description** attribute on the computer account in Active Directory. Select **Custom**, and add `Description` as a custom attribute. After this discovery method runs, this attribute shows on the device Properties tab in the Configuration Manager console.

4. On the **Options** tab, configure settings to filter out or exclude stale computer records from discovery.
5. Select **OK** to save the configuration.

Configure Active Directory User Discovery

1. On the **General** tab of the Active Directory User Discovery Properties window, select the **New** icon to specify a new Active Directory container. In the **Active Directory Container** dialog box, finish the following configurations:

   a. Specify one or more locations to search.

   b. For each location, specify options that change the search behavior.

   c. For each location, specify the account to use as the **Active Directory Discovery Account**. For more information, see Accounts.

> **NOTE**
> For each specified location, you can configure a unique set of discovery options and a unique Active Directory Discovery Account.

   d. Select **OK** to save the Active Directory container configuration.

2. On the **Polling Schedule** tab, configure both the full discovery polling schedule and delta discovery.
3. On the **Active Directory Attributes** tab, configure additional Active Directory attributes for computers that you want to discover. This tab lists the default object attributes.
4. Select **OK** to save the configuration.

Azure AD User Discovery

Azure AD User Discovery isn't enabled or configured the same as other discovery methods. Configure it when you onboard the Configuration Manager site to Azure AD.

For more information, see Azure AD User Discovery.

Prerequisites

To enable and configure this discovery method, Configure Azure Services for **Cloud Management**.

If you use Configuration Manager to *create* the Azure app, it configures the app with the necessary permissions.

If you create the app in Azure first, and then *import* it into Configuration Manager, you need to manually configure the app. This configuration includes granting the server app permission to read directory data.

1. Open the Azure portal as a user with *Global Admin* permissions. Go to **Azure Active Directory**, and select **App registrations**. Switch to **All applications** if necessary.
2. Select the target application.
3. In the **Manage** menu, select **API permissions**.
   a. On the **API permissions** panel, select **Add a permission**.
   b. In the **Request API permissions** panel, switch to **APIs my organization uses**.
   c. Search for and select the **Microsoft Graph** API.

> **TIP**
> In version 1810 and earlier, use the **Azure Active Directory Graph** API.

   d. Select the **Application permissions** group. Expand **Directory**, and select **Directory.Read.All**.
   e. Select **Add permissions**.
4. On the **API permissions** panel, in the **Grant consent** section, select **Grant admin consent...**. Select **Yes**.

Configure Azure AD User Discovery

When configuring the **Cloud Management** Azure service:

- On the **Discovery** page of the wizard, select the option to **Enable Azure Active Directory User Discovery**.
- Select **Settings**.
- In the Azure AD User Discovery Settings dialog box, configure a schedule for when discovery occurs. You can

also enable delta discovery, which only checks for new or changed accounts in Azure AD.

> **NOTE**
> If the user is a federated or synchronized identity, you must use Configuration Manager Active Directory user discovery as well as Azure AD user discovery. For more information about hybrid identities, see Define a hybrid identity adoption strategy.

Azure AD User Group Discovery

> **NOTE**
> In this version of Configuration Manager, Azure AD User Group Discovery is a pre-release feature. To enable it, see Pre-release features.

You can discover user groups and members of those groups from Azure AD. When the site finds users in Azure AD groups that it hasn't previously discovered, it adds them as new user resources in Configuration Manager. A user group resource record is created when the group is a security group.

Prerequisites

- Cloud Management Azure service
- Permission to read and search Azure AD groups

Limitations

Delta discovery for Azure AD user group discovery is currently disabled.

Log files

Use the SMS_AZUREAD_DISCOVERY_AGENT.log for troubleshooting. This log is also shared with Azure AD user discovery. For more information, see Log files.

Enable Azure AD user group discovery

To enable discovery on an existing **Cloud Management** Azure service:

1. Go to the **Administration** workspace, expand **Cloud Services**, then select the **Azure Services** node.
2. Select one of your Azure services, then select **Properties** in the ribbon.
3. In the **Discovery** tab, check the box to **Enable Azure Active Directory Group Discovery**, then select **Settings**.
4. Select **Add** under the **Discovery Scopes** tab.
   - You can modify the **Polling Schedule** in the other tab.
5. Select one or more user groups. You can **Search** by name and choose if you want to see **Security groups only**.
   - You'll be prompted to sign in to Azure when you select **Search** the first time.
6. Select **OK** when you finish selecting groups.
7. Once discovery finishes running, you can browse your Azure AD user groups in the **Users** node.

To enable discovery when configuring a new **Cloud Management** Azure service:

- On the **Discovery** page of the wizard, select the option to **Enable Azure Active Directory Group Discovery**.
- Select **Settings**.
- In the Azure AD Group Discovery Settings dialog box, configure your discovery scope and a schedule for when discovery occurs.

Heartbeat Discovery

Configuration Manager enables the Heartbeat Discovery method when you install a primary site. If you want to use the default schedule of every seven days, there's nothing else to configure. Otherwise, you only have to configure the schedule for how often clients send the Heartbeat Discovery data record to a management point.

> **NOTE**
> If you enable both client push installation and the site maintenance task for **Clear Install Flag** at the same site, set the schedule of Heartbeat Discovery to be less than the **Client Rediscovery period** of the **Clear Install Flag** site maintenance task. For more information about site maintenance tasks, see Maintenance tasks.

Configure the Heartbeat Discovery schedule

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Hierarchy Configuration**, and select the **Discovery Methods** node.
2. Select the **Heartbeat Discovery** method for the site where you want to configure Heartbeat Discovery.
3. On the **Home** tab of the ribbon, select **Properties**.
4. Configure the frequency with which clients submit a Heartbeat discovery data record. Then select **OK** to save the configuration.

Network Discovery

Before you configure Network Discovery, understand the following topics:

- Available levels of Network Discovery
- Available Network Discovery options
- Limiting Network Discovery on the network

For more information, see About Network Discovery.

The following sections provide information about common configurations for Network Discovery. You can configure one or more of these configurations for use during the same discovery run. If you use multiple configurations, plan for the interactions that can affect the discovery results.

For example, you discover all Simple Network Management Protocol (SNMP) devices that use a specific SNMP community name. For the same discovery run, you disable discovery on a specific subnet. When discovery runs, Network Discovery doesn't discover the SNMP devices with the specified community name on the subnet that you've disabled.

Determine your network topology

You can use a topology-only discovery to map your network. This kind of discovery doesn't discover potential clients. The topology-only Network Discovery relies on SNMP.

When you're mapping your network topology, configure the**Maximum hops** on the **SNMP** tab in the **Network Discovery Properties** dialog box. Just a few hops can help control the network bandwidth that's used when discovery runs. As you discover more of your network, increase the number of hops to gain a better understanding of your network topology.

After you understand your network topology, configure additional properties for Network Discovery. These properties help to discover potential clients and their operating systems. Also configure Network Discovery to limit the network segments that it can search.

For more information, see How to determine your network topology

Network Discovery search options

Configuration Manager supports the following methods to search the network:

- Limit searches by using subnets
- Search a specific domain
- Limit searches by using SNMP community names
- Search a specific DHCP server

Limit searches by using subnets

You can configure Network Discovery to search specific subnets during a discovery run. By default, Network Discovery searches the subnet of the server that runs discovery. Any additional subnets that you configure and enable apply only to SNMP and DHCP search options. When Network Discovery searches domains, it isn't limited by configurations for subnets.

If you specify one or more subnets on the **Subnets** tab in the **Network Discovery Properties** dialog box, it only searches the subnets that you mark as **Enabled**.

When you disable a subnet, the site excludes it from discovery, and the following conditions apply:

- SNMP-based queries don't run on the subnet.
- DHCP servers don't reply with a list of resources located on the subnet.
- Domain-based queries can discover resources that are located on the subnet.

Search a specific domain

You can configure Network Discovery to search a specific domain or set of domains during a discovery run. By default, Network Discovery searches the local domain of the server that runs discovery.

If you specify one or more domains on the **Domains** tab in the **Network Discovery Properties** dialog box, it only searches the domains that you mark as **Enabled**.

When you disable a domain, the site excludes it from discovery, and the following conditions apply:

- Network Discovery doesn't query domain controllers in that domain.
- SNMP-based queries can still run on subnets in the domain.
- DHCP servers can still reply with a list of resources located in the domain.

Limit searches by using SNMP community names

You configure Network Discovery to search a specific SNMP community or set of communities during a discovery run. By default, the method configures the **public** community name.

Network Discovery uses community names to gain access to routers that are SNMP devices. A router can supply Network Discovery with information about other routers and subnets that are linked to the first router.

> **NOTE**
>
> SNMP community names resemble passwords. Network Discovery can get information only from an SNMP device for which you've specified a community name. Each SNMP device can have its own community name, but often the same community name is shared among several devices. Additionally, most SNMP devices have a default community name of **public**. But some organizations delete the **public** community name from their devices as a security precaution.

If you include more than one SNMP community on the **SNMP** tab in the **Network Discovery Properties** dialog box, it searches them in the order in which they're shown. Make sure that the most frequently used names are at the top of the list. This configuration helps to minimize network traffic that the site generates when it tries to contact a device by using different names.

> **NOTE**
>
> Along with using the SNMP community name, you can specify the IP address or resolvable name of a specific SNMP device. You do this action on the **SNMP Devices** tab in the **Network Discovery Properties** dialog box.

Search a specific DHCP server

You can configure Network Discovery to use a specific DHCP server or multiple servers to discover DHCP clients during a discovery run.

Network Discovery searches each DHCP server that you specify on the **DHCP** tab in the **Network Discovery Properties** dialog box. If the server that's running discovery leases its IP address from a DHCP server, you can configure discovery to search that DHCP server. Enable this behavior with the option to **Include the DHCP server that the site server is configured to use**.

> **NOTE**
>
> To successfully configure a DHCP server in Network Discovery, your environment must support IPv4. You can't configure Network Discovery to use a DHCP server in a native IPv6 environment.

How to configure Network Discovery

Use the following procedures to first discover only your network topology, and then to configure Network Discovery to discover potential clients by using one or more of the available Network Discovery options.

How to determine your network topology

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Hierarchy Configuration**, and select the **Discovery Methods** node.
2. Select the **Network Discovery** method for the site where you want to discover network resources.
3. On the **Home** tab of the ribbon, select **Properties**.
   - On the **General** tab, select the option to **Enable network discovery**. Then select **Topology** from the **Type of discovery** options.
   - On the **Subnets** tab, select the **Search local subnets** option.

     > **TIP**
     >
     > If you know the specific subnets that constitute your network, deselect the **Search local subnets** checkbox. Then select the **New** icon  , and add the specific subnets that you want to search. For large networks, search only one or two subnets at a time to minimize the use of network bandwidth.

   - On the **Domains** tab, select the option to **Search local domain**.
   - On the **SNMP** tab, select an option from the **Maximum hops** drop-down list. This option specifies how many router hops Network Discovery can take in mapping your topology.

     > **TIP**
     >
     > When you first map your network topology, configure just a few router hops to minimize the use of network bandwidth.

4. On the **Schedule** tab, select the **New** icon  , and set a schedule for running discovery.

> **NOTE**
> You can't assign a different discovery configuration to separate Network Discovery schedules. Each time Network Discovery runs, it uses the current discovery configuration.

5. Select **OK** to accept the configurations. Network Discovery runs at the scheduled time.

How to configure Network Discovery

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Hierarchy Configuration**, and select the **Discovery Methods** node.
2. Select the **Network Discovery** method for the site where you want to discover network resources.
3. On the **Home** tab of the ribbon, select **Properties**.
4. On the **General** tab, select the option to **Enable network discovery**.
   - Select from the **Type of discovery** options the type of discovery that you want to run.
   - Enable the **Slow network** option for Configuration Manager to make automatic adjustments for low-bandwidth networks.
5. To configure discovery to search subnets, switch to the **Subnets** tab. Then configure one or more of the following options:
   - To run discovery on subnets that are local to the computer that runs discovery, enable the option to **Search local subnets**.
   - To search a specific subnet, make sure that the subnet is listed in **Subnets to search** and has a **Search** value of **Enabled**:
     a. If the subnet isn't listed, select the **New** icon  . In the **New Subnet Assignment** dialog box, enter the **Subnet** and **Mask** information, and then select **OK**. By default, a new subnet is enabled for search.
     b. To change the **Search** value for a listed subnet, select it in the list. Then select the **Toggle** icon to switch the value between **Disabled** and **Enabled**.
6. To configure discovery to search domains, switch to the **Domains** tab. Then configure one or more of the following options:
   - To run discovery on the domain of the computer that runs discovery, enable the option to **Search local domain**.
   - To search a specific domain, make sure that the domain is listed in **Domains** and has a **Search** value of **Enabled**:
     a. If the domain isn't listed, select the **New** icon  . In the **Domain Properties** dialog box, enter the **Domain** information, and then select **OK**. By default, a new domain is enabled for search.
     b. To change the **Search** value for a listed domain, select it in the list. Then select the **Toggle** icon to switch the value between **Disabled** and **Enabled**.
7. To configure discovery to search specific SNMP community names for SNMP devices, switch to the **SNMP** tab. Then configure one or more of the following options:
   - To add an SNMP community name to the list of **SNMP Community names**, select the **New** icon  . In the **New SNMP Community Name** dialog box, specify the **Name** of the SNMP community, and then select **OK**.

- To remove an SNMP community name, select the community name, and then select the **Delete** icon  .
- To adjust the search order of SNMP community names, select a community name from the list. Then select the **Move Item Up** icon  or the **Move Item Down** icon  . When discovery runs, community names are searched in a top-to-bottom order.
- To configure the maximum number of router hops for use by SNMP searches, select the number of hops from the **Maximum hops** drop-down list.

8. To configure an SNMP device, switch to the **SNMP Devices** tab. If the device isn't listed, select the **New** icon  . In the **New SNMP Device** dialog box, specify the IP address or device name of the SNMP device, and then select **OK**.

   > **NOTE**
   > If you specify a device name, Configuration Manager must be able to resolve the NetBIOS name to an IP address.

9. To configure discovery to query specific DHCP servers, switch to the **DHCP** tab. Then configure one or more of the following options:

   - To query the DHCP server on the computer that is running discovery, enable the option to **Always use the site server's DHCP server**.

     > **NOTE**
     > To use this option, the server must lease its IP address from a DHCP server and can't use a static IP address.

   - To query a specific DHCP server, select the **New** icon  . In the **New DHCP Server** dialog box, specify the IP address or server name of the DHCP server, and then select **OK**.

     > **NOTE**
     > If you specify a server name, Configuration Manager must be able to resolve the NetBIOS name to an IP address.

10. To configure when discovery runs, switch to the **Schedule** tab. Then select the **New** icon  to set a schedule for running Network Discovery. You can configure multiple recurring schedules, and multiple schedules that have no recurrence.

    > **NOTE**
    > If the **Schedule** tab shows more than one schedule at the same time, Network Discovery runs for all schedules as it's configured at the time indicated in the schedule. This behavior is also true for recurring schedules.

11. Select **OK** to save your configurations.

How to verify that Network Discovery has finished

The time that Network Discovery requires to finish can vary depending on one or more of the following factors:

- The size of your network
- The topology of your network

- The maximum number of hops that are configured to find routers in the network
- The type of discovery that is being run

Network Discovery doesn't create messages to alert you when it's finished. Use the following procedure to verify when discovery has finished:

1. In the Configuration Manager console, go to the **Monitoring** workspace. Expand **System Status**, and then select the **Status Message Queries** node.
2. Select the **All Status Messages** query.
3. On the **Home** tab of the ribbon, in the **Status Message Queries** group, select **Show Messages**.
4. In the All Status Messages window, select a value from the **Select date and time** drop-down list that includes how long ago the discovery started. Then select **OK** to open the **Configuration Manager Status Message Viewer**.

   > **TIP**
   > You can also use the **Specify date and time** option to select a given date and time that you ran discovery. This option is useful when you ran Network Discovery on a given date and want to retrieve messages from only that date.

5. To validate that Network Discovery has finished, search for a status message that has the following details:
   - Message ID: **502**
   - Component: **SMS_NETWORK_DISCOVERY**
   - Description: **This component stopped**

   If this status message isn't present, Network Discovery hasn't finished.
6. To validate when Network Discovery started, search for a status message that has the following details:
   - Message ID: **500**
   - Component: **SMS_NETWORK_DISCOVERY**
   - Description: **This component started**

   This information verifies that Network Discovery started. If this information isn't present, reschedule Network Discovery.

Define site boundaries and boundary groups

6/18/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Boundaries in Configuration Manager define network locations on your intranet. These locations include devices that you want to manage. *Boundary groups* are logical groups of boundaries that you configure.

A hierarchy can include any number of boundary groups. Each boundary group can contain any combination of the following boundary types:

- IP subnet
- Active Directory site name
- IPv6 prefix
- IP address range

Clients on the intranet evaluate their current network location and then use that information to identify boundary groups to which they belong.

Clients use boundary groups to:

- **Find an assigned site:** Boundary groups enable clients to find a primary site for client assignment. This behavior is also known as *automatic site assignment*.
- **Find certain site system roles they can use:** Associate a boundary group with certain site system roles. Then the site provides clients with that list of site systems in the boundary group. Clients use these site systems for actions such as finding content or a nearby management point.

Clients that are on the internet or configured as internet-only clients don't use boundary information. These clients can't use automatic site assignment. They can download content from an internet-based distribution point from their assigned site or a cloud-based distribution point.

Starting in version 1902, you can associate a cloud management gateway (CMG) with a boundary group. For more information, see CMG hierarchy design.

Recommendations

Use a mix of the fewest boundaries that meet your needs

Use whichever boundary type or types you choose that work for your environment. To simplify your management tasks, use boundary types that let you use the fewest number of boundaries you can.

Avoid overlapping boundaries for automatic site assignment

Although each boundary group supports both site assignment and site system reference, create a separate set of boundary groups to use only for site assignment. Make sure that each boundary in a boundary group isn't a member of another boundary group with a different site assignment.

- A single boundary can be included in multiple boundary groups
- Each boundary group can be associated with a different primary site for site assignment
- For a boundary that's a member of two different boundary groups with different site assignments, clients randomly select a site to join. This behavior might not be for the site you want the client to join. This configuration is called *overlapping boundaries*.

Overlapping boundaries isn't a problem for content location. It can be a useful configuration that provides clients additional resources or content locations they can use.

Next steps

- Define network locations as boundaries
- Configure boundary groups

Define network locations as boundaries for System Center Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager boundaries are locations on your network that contain devices that you want to manage. The boundary a device is on is equivalent to the Active Directory site, or network IP address that is identified by the Configuration Manager client that is installed on the device.

- You can manually create individual boundaries. However, Configuration Manager does not support the direct entry of a supernet as a boundary. Instead, use the IP address range boundary type.
- You can configure the Active Directory Forest Discovery method to auto-discover and create boundaries for each IP Subnet and Active Directory Site it discovers. When Active Directory Forest Discovery identifies a supernet that is assigned to an Active Directory site, Configuration Manager converts the supernet into an IP address range boundary.

It is not uncommon for a device to use an IP address that the Configuration Manager administrator is not aware of. When the network location of a device is in doubt, confirm what the device reports as its location by using the **IPCONFIG** command on the device.

When you create a boundary, it automatically receives a name that is based upon the type and scope of the boundary. You cannot modify this name. Instead, you can specify a description to help identify the boundary in the Configuration Manager console.

Each boundary is available for use by every site in your hierarchy. After a boundary has been created, you can modify its properties to do the following:

- Add the boundary to one or more boundary groups.
- Change the type or scope of the boundary.
- View the boundaries **Site Systems** tab to see which site system servers (distribution points, state migration points, and management points) are associated with the boundary.

To create a boundary

1. In the Configuration Manager console, click **Administration** > **Hierarchy Configuration** > **Boundaries**
2. On the **Home** tab, in the **Create** group, click **Create Boundary.**
3. On the **General** tab of the Create Boundary dialog box you can specific a **Description** to identify the boundary by a friendly name or reference.
4. Select a **Type** for this boundary:
   - If you select **IP Subnet**, you must specify a **Subnet ID** for this boundary.

     > **TIP**
     > You can specify the **Network** and **Subnet mask** to have the **Subnet ID** automatically specified. When you save the boundary, only the Subnet ID value is saved.

   - If you select **Active Directory site**, you must specify or **Browse** to an Active Directory site in the

local forest of the site server.

  - When you specify an Active Directory site for a boundary, the boundary includes each IP Subnet that is a member of that Active Directory site. If the configuration of the Active Directory site changes in Active Directory, the network locations included in this boundary also change.
  - Active Directory site boundaries do not work for pure AzureAD clients. If they roam on-premises they will not fall into any boundary if only defined using AD Sites.

- If you select **IPv6 prefix**, you must specify a **Prefix** in the IPv6 prefix format.
- If you select **IP address range**, you must specify a **Starting IP address** and **Ending IP address** that includes part of an IP Subnet or includes multiple IP Subnets.

5. Click **OK** to save the new boundary.

To configure a boundary

1. In the Configuration Manager console, click **Administration** > **Hierarchy Configuration** > **Boundaries**
2. Select the boundary you want to modify.
3. On the **Home** tab, in the **Properties** group, click **Properties**.
4. In the **Properties** dialog box for the boundary, select the **General** tab to edit the **Description** or **Type** for the boundary. You can also change the scope of a boundary by editing the network locations for the boundary. For example, for an Active Directory site boundary you can specify a new Active Directory site name.
5. Select the **Site Systems** tab to view the site systems that are associated with this boundary. You cannot change this configuration from the properties of a boundary.

   > **TIP**
   > For a site system server to be listed as a site system for a boundary, the site system server must be associated as a site system server for at least one boundary group that includes this boundary. This is configured on the **References** tab of a boundary group.

6. Select the **Boundary Groups** tab to modify the boundary group membership for this boundary:
   - To add this boundary to one or more boundary groups, click **Add**, select the check box for one or more boundary groups, and then click **OK**.
   - To remove this boundary from a boundary group, select the boundary group and click **Remove**.
7. Click **OK** to close the boundary properties and save the configuration.

Configure boundary groups for Configuration Manager

6/18/2019 • 27 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use boundary groups in Configuration Manager to logically organize related network locations (boundaries) to make it easier to manage your infrastructure. Assign boundaries to boundary groups before using the boundary group.

By default, Configuration Manager creates a default site boundary group at each site.

To configure boundary groups, associate boundaries (network locations) and site system roles, like distribution points, to the boundary group. This configuration helps associate clients to site system servers like distribution points that are located near the clients on the network.

To increase the availability of servers to a wider range of network locations, assign the same boundary and the same server to more than one boundary group.

Clients use a boundary group for:

- Automatic site assignment
- To find a site system server that can provide a service, including:
  - Distribution points for content location
  - Software update points
  - State migration points
  - Preferred management points
  - Cloud management gateway (starting in version 1902)

> **NOTE**
> If you use preferred management points, enable this option for the hierarchy, not from within the boundary group configuration. For more information, see Enable use of preferred management points.

Boundary groups and relationships

For each boundary group in your hierarchy, you can assign:

- One or more boundaries. A client's **current** boundary group is a network location that's defined as a boundary assigned to a specific boundary group. A client can have more than one current boundary group.
- One or more site system roles. Clients can always use roles associated with their current boundary group. Depending on additional configurations, they can use roles in additional boundary groups.

For each boundary group you create, you can configure a one-way link to another boundary group. The link is called a **relationship**. The boundary groups you link to are called **neighbor** boundary groups. A boundary group can have more than one relationship, each with a specific neighbor boundary group.

When a client fails to find an available site system in its current boundary group, the configuration of each

relationship determines when it begins to search a neighbor boundary group. This search of additional groups is called **fallback**.

For more information, see the following procedures:

- Create a boundary group
- Configure a boundary group

Fallback

To prevent problems when clients can't find an available site system in their current boundary group, define the relationship between boundary groups for fallback behavior. Fallback lets a client expand its search to additional boundary groups to find an available site system.

Relationships are configured on a boundary group properties **Relationships** tab. When you configure a relationship, you define a link to a neighbor boundary group. For each type of supported site system role, configure independent settings for fallback to the neighbor boundary group. For more information, see Configure fallback behavior.

For example, when you configure a relationship to a specific boundary group, set fallback for distribution points to occur after 20 minutes. The default is 120 minutes For a more extensive example, see Example of using boundary groups.

If a client fails to find an available site system role in its current boundary group, the client uses the fallback time in minutes. This fallback time determines when the client begins to search for an available site system associated with the neighbor boundary group.

When a client can't find an available site system, it begins to search locations from neighbor boundary groups. This behavior increases the pool of available site systems. The configuration of boundary groups and their relationships defines the client's use of this pool of available site systems.

- A boundary group can have more than one relationship. With this configuration, you can configure fallback for each type of site system to different neighbors to occur after different periods of time.
- Clients only fall back to a boundary group that's a direct neighbor of their current boundary group.
- When a client is a member of more than one boundary group, it defines its current boundary group as a union of all its boundary groups. The client falls back to neighbors of any of those original boundary groups.

The default site boundary group

You can create your own boundary groups, and each site has a default site boundary group that Configuration Manager creates. This group is named **Default-Site-Boundary-Group<sitecode>**. For example, the group for site ABC would be named **Default-Site-Boundary-Group<ABC>**.

For each boundary group you create, Configuration Manager automatically creates an implied link to each default site boundary group in the hierarchy.

- The implied link is a default fallback option from a current boundary group to the site's default boundary group. The default fallback time is 120 minutes.
- For clients not in a boundary associated with any boundary group: to identify valid site system roles, use the default site boundary group from their assigned site.

To manage fallback to the default site boundary group:

- Open the properties of the site default boundary group, and change the values on the **Default Behavior** tab. Changes you make here apply to *all* implied links to this boundary group. When you configure an explicit link to this default site boundary group from another boundary group, you override these default

settings.

- Open the properties of a custom boundary group. Change the values for the explicit link to a default site boundary group. When you set a new time in minutes for fallback or block fallback, that change affects only the link you're configuring. Configuration of the explicit link overrides the settings on the **Default Behavior** tab of a default site boundary group.

Site assignment

You can configure each boundary group with an assigned site for clients.

- A newly installed client that uses automatic site assignment joins the assigned site of a boundary group that contains the client's current network location.
- After assigning to a site, a client doesn't change its site assignment when it changes its network location. For example, a client roams to a new network location. This location is a boundary in a boundary group with a different site assignment. The client's assigned site doesn't change.
- When Active Directory System Discovery discovers a new resource, the site evaluates network information for the resource against the boundaries in boundary groups. This process associates the new resource with an assigned site for use by the client push installation method.
- When a boundary is a member of more than one boundary groups that have different assigned sites, clients randomly select one of the sites.
- Changes to a boundary groups assigned site only apply to new site assignment actions. Clients that previously assigned to a site don't reevaluate their site assignment based on changes to the configuration of a boundary group (or to their own network location).

For more information about client site assignment, see Using automatic site assignment for computers.

For more information on how to configure site assignment, see the following procedures:

- Configure site assignment and select site system servers
- Configure a fallback site for automatic site assignment

Distribution points

When a client requests the location of a distribution point, Configuration Manager sends the client a list of site systems. These site systems are of the appropriate type associated with each boundary group that includes the client's current network location:

- **During software distribution**, clients request a location for deployment content on a valid content source. This location may be a distribution point, or a peer cache source.
- **During OS deployment**, clients request a location to send or receive their state migration information.
    - Starting in version 1810, clients acquire content based on boundary group behaviors. For more information, see Task sequence support for boundary groups.

During content deployment, if a client requests content that isn't available from a source in its current boundary group, the client continues to request that content. The client tries different content sources in its current boundary group until it reaches the fallback period for a neighbor or the default site boundary group. If the client still hasn't found content, it then expands its search for content sources to include the neighbor boundary groups.

If you configure the content to distribute on-demand, and it isn't available on a distribution point when a client requests it, the site begins to transfer the content to that distribution point. It's possible the client finds that server as a content source before falling back to use a neighbor boundary group.

Client installation

When installing the Configuration Manager client, the ccmsetup process contacts the management point to locate the necessary content. During this process in versions 1806 and earlier, the management point only returns distribution points in the client's current boundary group. If no content is available, the setup process falls back to download content from the management point. There's no option to fall back to distribution points in other boundary groups that might have the necessary content.

Starting in version 1810, the management point returns distribution points based on boundary group configuration. If you define relationships on the boundary group, the management point returns distribution points in the following order:

1. Current boundary group
2. Neighbor boundary groups
3. The site default boundary group

> **NOTE**
> The client setup process doesn't use the fallback time. To locate content as quickly as possible, it immediately falls back to the next boundary group.

Task sequence support for boundary groups

Starting in version 1810, when a device runs a task sequence and needs to acquire content, it now uses boundary group behaviors similar to the Configuration Manager client.

Configure this behavior using the following settings on the **Distribution Points** page of the task sequence deployment:

- **When no local distribution point is available, use a remote distribution point**: For this deployment, the task sequence can fall back to distribution points in a neighbor boundary group.
- **Allow clients to use distribution points from the default site boundary group**: For this deployment, the task sequence can fall back to distribution points in the default site boundary group.

To use this new behavior, make sure to update clients to the latest version.

Location priority

The task sequence tries to acquire content in the following order:

1. Peer cache sources
2. Distribution points in the *current* boundary group
3. Distribution points in a *neighbor* boundary group

   > **IMPORTANT**
   > Due to the real-time nature of task sequence processing, it doesn't wait for the failover time on a neighbor boundary group. It uses the failover times for prioritizing the neighbor boundary groups. For example, if the task sequence fails to acquire content from a distribution point in its current boundary group, it immediately tries a distribution point in a neighbor boundary group with the shortest failover time. If that process fails, it then fails over to a distribution point in a neighbor boundary group with a larger failover time.

4. Distribution points in the *site default* boundary group

The task sequence log file **smsts.log** shows the priority of the location sources that it uses based on the deployment properties.

Boundary group options for peer downloads

Starting in version 1806, boundary groups include the following additional settings to give you more control over content distribution in your environment:

- Allow peer downloads in this boundary group
- During peer downloads, only use peers within the same subnet

Version 1810 adds the following options:

- Prefer distribution points over peers with the same subnet
- Prefer cloud distribution points over distribution points

For more information on how to configure these settings, see Configure a boundary group.

Allow peer downloads in this boundary group

This setting is enabled by default. The management point provides clients a list of content locations that includes peer sources. This setting also affects applying Group IDs for Delivery Optimization.

There are two common scenarios in which you should consider disabling this option:

- If you have a boundary group that includes boundaries from geographically dispersed locations such as a VPN. Two clients may be in the same boundary group because they're connected through VPN, but in vastly different locations that are inappropriate for peer sharing of content.
- If you use a single, large boundary group for site assignment that doesn't reference any distribution points.

During peer downloads, only use peers within the same subnet

This setting is dependent upon the preceding option. If you enable this option, the management point only includes in the content location list peer sources that are in the same subnet as the client.

Common scenarios for enabling this option:

- Your boundary group design for content distribution includes one large boundary group that overlaps other smaller boundary groups. With this new setting, the list of content sources that the management point provides to clients only includes peer sources from the same subnet.
- You have a single large boundary group for all remote office locations. Enable this option and clients only share content within the subnet at the remote office location, instead of risking sharing content between locations.

Prefer distribution points over peers with the same subnet

By default, the management point prioritizes peer cache sources at the top of the list of content locations. This setting reverses that priority for clients that are in the same subnet as the peer cache source.

Prefer cloud distribution points over distribution points

If you have a branch office with a faster internet link, you can now prioritize cloud content.

In version 1902, this setting is now titled **Prefer cloud based sources over on-premise sources**. The behavior remains the same.

Software update points

Clients use boundary groups to find a new software update point. To control which servers a client can find, add individual software update points to different boundary groups.

If you update from a version prior to 1702, each site adds all existing software update points to the default site boundary group. This site update behavior maintains the prior client behavior to select a software update point from the pool of available servers. This behavior is maintained until you choose to add individual software update

points to different boundary groups for controlled selection and fallback behavior.

If you install a new site, software update points aren't added to the default site boundary group. Assign software update points to a boundary group so that clients can find and use them.

Fallback for software update points

Fallback for software update points is configured like other site system roles, but has the following caveats:

New clients use boundary groups to select software update points

When you install new clients, they select a software update point from those servers associated with the boundary groups you configure. This behavior replaces the previous behavior where clients select a software update point randomly from a list of the servers that share the client's forest.

Clients continue to use a last known-good software update point until they fallback to find a new one

Clients that already have a software update point continue to use it until it can't be reached. This behavior includes continued use of a software update point that isn't associated with the client's current boundary group.

This behavior is intentional. The client continues to use an existing software update point, even when it isn't in the client's current boundary group. When the software update point changes, the client synchronizes data with the new server, which causes significant network usage. If all clients switch to a new server at the same time, the delay in transition helps to avoid saturating your network.

A client always tries to reach its last known-good software update point for 120 minutes before starting fallback

After 120 minutes, if the client hasn't established contact, it then begins fallback. When fallback starts, the client receives a list of all software update points in its current boundary group. Additional software update points in neighbor and site default boundary groups are available based on fallback configurations.

Fallback configurations for software update points

You can configure **Fallback times (in minutes)** for software update points to be less than 120 minutes. However, the client still tries to reach its original software update point for 120 minutes. Then it expands its search to additional servers. Boundary group fallback times start when the client first fails to reach its original server. When the client expands its search, the site provides any boundary groups configured for less than 120 minutes.

To block fallback for a software update point to a neighbor boundary group, configure the setting to **Never fallback**.

After failing to reach its original server for two hours, the client then uses a shorter cycle to establish a connection to a new software update point. This behavior enables the client to rapidly search through the expanding list of potential software update points.

Example

You configure software update points in boundary group *A* to fallback after **10** minutes. You configure the same setting for boundary group *B* to **130** minutes. A client in boundary group *Z* fails to reach its last known-good software update point.

- For the next 120 minutes, the client tries to reach only its original server in boundary group Z. After 10 minutes, Configuration Manager adds the software update points from boundary group A to the pool of available servers. However, the client doesn't try to contact them or any other server until the initial 120-minute period elapses.
- After trying to contact the original software update point for 120 minutes, the client expands its search. It adds servers to the available pool of software update points that are in it's current and any neighbor boundary groups configured for 120 minutes or less. This pool includes the servers in boundary group A, which were previously added to the pool of available servers.
- After 10 more minutes, the client expands the search to include software update points from boundary group B. This period is 130 minutes of total time after the client first failed to reach its last known-good software update point.

Manually switch to a new software update point

Along with fallback, use client notification to manually force a device to switch to a new software update point.

When you switch to a new server, the devices use fallback to find that new server. Clients switch to the new software update point during their next software updates scan cycle.

Review your boundary group configurations. Before you start this change, make sure that your software update points are in the correct boundary groups.

For more information, see Manually switch clients to a new software update point.

Management points

Starting in version 1802, configure fallback relationships for management points between boundary groups. This behavior provides greater control for the management points that clients use. On the **Relationships** tab of the boundary group properties, there's a column for management point. When you add a new fallback boundary group, the fallback time for the management point is currently always zero (0). This behavior is the same for the **Default Behavior** on the site default boundary group.

Previously, a common problem occurs when you have a protected management point in a secure network. Clients on the main corporate network receive policy that includes this protected management point, even though they can't communicate with it across a firewall. To address this problem, use the **Never fallback** option to make sure that clients only fallback to management points with which they can communicate.

When upgrading the site to version 1802, Configuration Manager adds all intranet management points into the site default boundary group. (This group of servers doesn't include management points that are only internet-facing.) This upgrade behavior makes sure that older client versions continue to communicate with management points. To take full advantage of this feature, move your management points to the desired boundary groups.

> **NOTE**
> If you enable distribution points in the site default boundary group to fallback, and a management point is colocated on a distribution point, the site also adds that management point to the site default boundary group.

If a client is in a boundary group that with no assigned management point, the site gives the client the entire list of management points. This behavior makes sure that a client always receives a list of management points.

Management point boundary group fallback doesn't change the behavior during client installation (ccmsetup.exe). If the command line doesn't specify the initial management point using the /MP parameter, the new client receives the full list of available management points. For its initial bootstrap process, the client uses the first management point it can access. Once the client registers with the site, it receives the management point list properly sorted with this new behavior.

For more information on the client's behavior to acquire content during installation, see Client installation.

During client upgrade, if you don't specify the /MP command-line parameter, the client queries sources such as Active Directory and WMI for any available management point. Client upgrade doesn't honor the boundary group configuration.

For clients to use this capability, enable the following setting: **Clients prefer to use management points specified in boundary groups** in **Hierarchy Settings**.

> **NOTE**
> OS deployment processes aren't aware of boundary groups for management points.

Troubleshooting

New entries appear in the **LocationServices.log**. The **Locality** attribute identifies one of the following states:

- **0**: Unknown
- **1**: The specified management point is only in the site default boundary group for fallback
- **2**: The specified management point is in a remote or neighbor boundary group. When the management point is in both a neighbor and the site default boundary groups, the locality is 2.
- **3**: The specified management point is in the local or current boundary group. When the management point is in the current boundary group and either a neighbor or the site default boundary group, the locality is 3. If you don't enable the preferred management points setting in Hierarchy Settings, the locality is always 3 no matter which boundary group the management point is in.

Clients use local management points first (locality 3), remote second (locality 2), then fallback (locality 1).

When a client receives five errors in 10 minutes and fails to communicate with a management point in its current boundary group, it tries to contact a management point in a neighbor or the site default boundary group. If the management point in the current boundary group later comes back online, the client returns to the local management point on the next refresh cycle. The refresh cycle is 24 hours, or when the Configuration Manager agent service restarts.

Preferred management points

> **NOTE**
> The behavior of this hierarchy setting, **Clients prefer to use management points specified in boundary groups**, changes starting in version 1802. When you enable this setting, Configuration Manager uses the boundary group functionality for the assigned management point. For more information, see management points.

Preferred management points enable a client to identify a management point that's associated with its current network location (boundary).

- A client tries to use a preferred management point from its assigned site before using one not configured as preferred from its assigned site.
- To use this option, enable **Clients prefer to use management points specified in boundary groups** in **Hierarchy Settings**. Then configure boundary groups at individual primary sites. Include the management points that should be associated with that boundary group's associated boundaries. For more information, see Enable use of preferred management points.
- When you configure preferred management points, and a client organizes its list of management points, the client places the preferred management points at the top of its list. This list includes all management points from the client's assigned site.

> **NOTE**
> Client roaming means it changes its network locations. For example, when a laptop travels to a remote office location. When a client roams, it might use a management point from the local site before attempting to use a server from its assigned site. This list of servers from its assigned site includes the preferred management points. For more information, see Understand how clients find site resources and services.

Overlapping boundaries

Configuration Manager supports overlapping boundary configurations for content location. When the client's network location belongs to more than one boundary group:

- When a client requests content, Configuration Manager sends the client a list of all distribution points that have the content.
- When a client requests a server to send or receive its state migration information, Configuration Manager sends the client a list of all state migration points associated with a boundary group that includes the current network location of the client.

This behavior enables the client to select the nearest server from which to transfer the content or state migration information.

Example of using boundary groups

The following example uses a client searching for content from a distribution point. This example can be applied to other site system roles that use boundary groups.

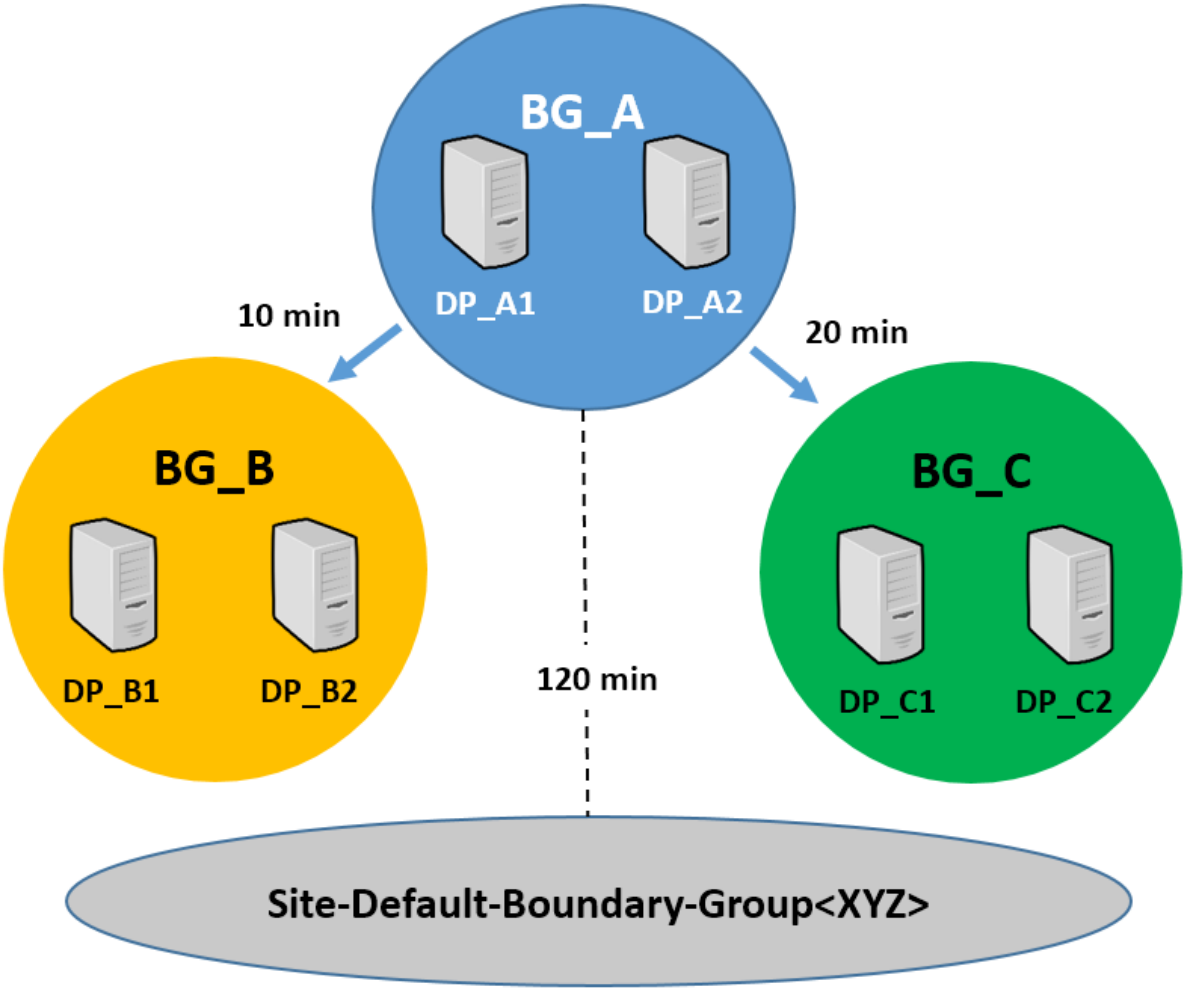
Create three boundary groups that don't share boundaries or site system servers:

- Group BG_A with distribution points DP_A1 and DP_A2
- Group BG_B with distribution points DP_B1 and DP_B2
- Group BG_C with distribution points DP_C1 and DP_C2

Add the network locations of your clients as boundaries to only the BG_A boundary group. Then configure relationships from that boundary group to the other two boundary groups:

- Configure distribution points for the first *neighbor* group (BG_B) to be used after 10 minutes. This group contains distribution points DP_B1 and DP_B2. Both are well connected to the first group's boundary locations.
- Configure the second *neighbor* group (BG_C) to be used after 20 minutes. This group contains distribution points DP_C1 and DP_C2. Both are across a WAN from the other two boundary groups.
- Also add to the default site boundary group another distribution point that's on the site server. This server is your least preferred content source location, but it's centrally located to all your boundary groups.

  Example of boundary groups and fallback times:



With this configuration:

- The client begins searching for content from distribution points in its *current* boundary group (BG_A). It searches each distribution point for two minutes, and then switches to the next distribution point in the boundary group. The client's pool of valid content source locations includes DP_A1 and DP_A2.
- If the client fails to find content from its *current* boundary group after searching for 10 minutes, it then adds the distribution points from the BG_B boundary group to its search. It then continues to search for content from a distribution point in its combined pool of servers. This pool now includes servers from both the BG_A and BG_B boundary groups. The client continues to contact each distribution point for two minutes, and then switches to the next server in its pool. The client's pool of valid content source locations includes DP_A1, DP_A2, DP_B1, and DP_B2.
- After an additional 10 minutes (20 minutes total), if the client still hasn't found a distribution point with content, it expands its pool to include available servers from the second *neighbor* group, boundary group BG_C. The client now has six distribution points to search: DP_A1, DP_A2, DP_B2, DP_B2, DP_C1, and DP_C2. It continues changing to a new distribution point every two minutes until it finds content.
- If the client hasn't found content after a total of 120 minutes, it falls back to include the *default site boundary group* as part of its continued search. Now the pool includes all distribution points from the three configured boundary groups, and the final distribution point located on the site server. The client then continues its search for content, changing distribution points every two minutes until content is found.

By configuring the different neighbor groups to be available at different times, you control when specific distribution points are added as a content source location. The client uses fallback to the default site boundary group as a safety net for content that isn't available from any other location.

Changes from prior versions

The following are the key changes to boundary groups and how clients find content in Configuration Manager current branch. Many of these changes and concepts work together.

Configurations for Fast or Slow are removed

You no longer configure individual distribution points to be fast or slow. Instead, each site system associated with a boundary group is treated the same. Because of this change, the **References** tab of the boundary group properties no longer supports the configuration of Fast or Slow.

New default boundary group at each site

Each primary site has a new default boundary group named **Default-Site-Boundary-Group<sitecode>**. When a client isn't on a network location assigned to a boundary group, it uses the site systems associated with the default group from its assigned site. Plan to use this boundary group as a replacement to the concept of fallback content location.

Allow fallback source locations for content is removed

You no longer explicitly configure a distribution point to be used for fallback. The options to configure this setting are removed from the console.

Additionally, the result of setting **Allow clients to use a fallback source location for content** on a deployment type for applications has changed. This setting on a deployment type now enables a client to use the default site boundary group as a content source location.

Boundary groups relationships

You can link each boundary group to one or more additional boundary groups. These links form relationships that you configure on the new boundary group properties tab named **Relationships**:

- Each boundary group that a client is directly associated with is called a **current** boundary group.
- Any boundary group a client can use because of an association between that client's *current* boundary group and another group is called a **neighbor** boundary group.
- On the **Relationships** tab, add boundary groups to use as a *neighbor* boundary group. Also configure a time in minutes for fallback. When a client fails to find content from a distribution point in the *current* group, this time is when the client begins to search content locations from *neighbor* boundary groups.

  When you add or change a boundary group configuration, you can block fallback to that specific boundary group from the current group you're configuring.

To use the new configuration, define explicit associations (links) from one boundary group to another. Configure all distribution points in that associated group with the same time in minutes. When a client fails to find a content source from its *current* boundary group, the time you configure determines when it begins to search for content sources from its neighbor boundary group.

In addition to boundary groups you explicitly configure, each boundary group has an implied link to the default site boundary group. This link becomes active after 120 minutes. Then the default site boundary group becomes a neighbor boundary group. This behavior allows the clients to use as content source locations the distribution points associated with that boundary group.

This behavior replaces what was previously referred to as fallback for content. Override this default behavior of 120 minutes by explicitly associating the default site boundary group to a *current* group. Set a specific time in minutes, or block fallback entirely to prevent its use.

Clients try to get content from each distribution point for up to two minutes

When a client searches for a content source location, it tries to access each distribution point for two minutes before then trying another distribution point. This behavior is a change from previous versions where clients tried

to connect to a distribution point for up to two hours.

- Clients randomly select the first distribution point from the pool of available servers in the client's *current* boundary group (or groups).
- After two minutes, if the client hasn't found the content, it switches to a new distribution point and tries to get content from that server. This process repeats every two minutes until the client finds the content or reaches the last server in its pool.
- If a client can't find a valid content source location from its *current* pool before it reaches the period for fallback to a *neighbor* boundary group, the client then adds the distribution points from that *neighbor* group to the end of its current list. It then searches the expanded group of source locations that includes the distribution points from both boundary groups.

  > **TIP**
  > When you create an explicit link from the current boundary group to the default site boundary group, and define a fallback time that is less than the fallback time for a link to a neighbor boundary group, clients begin searching source locations from the default site boundary group before including the neighbor group.

- When the client fails to get content from the last server in the pool, it begins the process again.

See also

- Procedures for boundary groups
- About boundaries
- Fundamental concepts for content management

How to configure boundary groups for Configuration Manager

5/9/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article includes procedures on how to configure boundary groups. Before you begin, make sure you understand boundary group concepts. For more information, see Boundary groups.

Create a boundary group

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Hierarchy Configuration**, and select the **Boundary Groups** node.
2. On the **Home** tab, in the **Create** group, select **Create Boundary Group**.
3. In the **Create Boundary Group** dialog box, on the **General** tab, specify a **Name** for this boundary group. Optionally include a **Description**.
4. Select **OK** to save the new boundary group, or continue to the next section to configure the boundary group.

Configure a boundary group

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Hierarchy Configuration**, and select the **Boundary Groups** node.
2. Select the boundary group you want to modify, and select **Properties** in the ribbon. This action opens the boundary group Properties window.

Configure the following settings:

- Add or remove boundaries
- Configure site assignment and select site system servers
- Configure fallback behavior
- Configure boundary group options

Add or remove boundaries

In the boundary group Properties window, use the **General** tab to modify the boundaries that are members of this boundary group:

- To add boundaries, select **Add**. In the Add Boundaries window, select the check box for one or more boundaries, and select **OK**.
- To remove boundaries, select the boundary in the list, and select **Remove**.

Configure site assignment and select site system servers

To modify the site assignment and associated site system server configuration, switch to the **References** tab in the boundary group Properties window.

- To enable this boundary group for use by clients for site assignment, select **Use this boundary group for site assignment**. Then select a site from the **Assigned site** dropdown list. For more information, see Site

assignment.

- To associate available site system servers with this boundary group, select **Add**. The Add Site Systems window only lists servers that have supported site system roles. Select the check box for one or more servers, and select **OK**. It adds them as associated site system servers for this boundary group.

  > **NOTE**
  > You can select any combination of available site systems from any site in the hierarchy. Selected site systems are listed on the **Site Systems** tab in the properties of each boundary that's a member of this boundary group.

- To remove a server from this boundary group, select the server and then select **Remove**.

  > **NOTE**
  > To stop use of this boundary group for associating site systems, remove all servers listed as associated site system servers.

Configure fallback behavior

To configure fallback behavior, switch to the **Relationships** tab in the boundary group Properties window.

- To create a relationship with another boundary group:
  - Select **Add**. In the Fallback Boundary Groups window, select the boundary group to configure.
  - Set a fallback time for the following site system roles:
    - Distribution point
    - Software update point
    - Management point

    > **NOTE**
    > For example, you open the Properties window for the Branch Office boundary group. In the Fallback Boundary Groups window, you select the Main Office boundary group. You set the distribution point fallback time to `20`. When you save this configuration, clients in the Branch Office boundary group will start searching for content from the distribution points in the Main Office boundary group after 20 minutes.

  - To prevent fallback to a specific boundary group, select the boundary group, and then select **Never fallback** for the type of site system role. This action can include the *default site boundary group*.
- To modify the configuration of an existing relationship, select the boundary group in the list, and select **Change**. This action opens the Fallback Boundary Groups window for just this boundary group.
- To remove a relationship, select the boundary group in the list, and select **Remove**.

For more information, see Fallback.

Configure boundary group options

Starting in version 1806, to configure additional options for clients in this boundary group, switch to the **Options** tab. For more information, see Boundary group options for peer downloads.

- **Allow peer downloads in this boundary group**: This option is enabled by default. The management point provides clients a list of content locations that includes peer sources.

- **During peer downloads, only use peers within the same subnet**: This setting is dependent upon the one above. If you enable this option, the management point only includes in the content location list peer sources that are in the same subnet as the client.

Configure a fallback site for automatic site assignment

If clients aren't in a boundary group with an assigned site, assign them to this site when they're installed.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. On the **Home** tab of the ribbon, in the **Sites** group, select **Hierarchy Settings**.
3. On the **General** tab, select the checkbox to **Use a fallback site**. Then select a site from the **Fallback site** drop-down list.
4. Select **OK** to save the configuration.

For more information, see Site assignment.

Enable use of preferred management points

For more information, see Preferred management points.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. On the **Home** tab of the ribbon, in the **Sites** group, select **Hierarchy Settings**.
3. On the **General** tab, select **Clients prefer to use management points specified in boundary groups**.
4. Select **OK** to save the configuration.

High availability options for Configuration Manager

7/26/2019 • 14 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article describes how to deploy Configuration Manager using options that maintain a high level of available service.

The following Configuration Manager options support high availability:

- Starting in version 1806, configure any standalone primary site with an additional site server in passive mode.
- Configure a SQL Server Always On availability group for the site database at primary sites and the central administration site.
- Sites support multiple instances of site system roles that provide important services to clients. For example, management points and distribution points.
- Central administration sites and primary sites support the backup of the site database. The site database stores all the configurations for sites and clients. The sites in a hierarchy share this configuration data.
- Built-in site recovery options can reduce server downtime. These advanced options simplify recovery when you have a hierarchy with a central administration site.
- Clients can automatically remediate typical issues without administrative intervention.
- Sites generate alerts about clients that fail to submit recent data, which alerts administrators to potential problems.
- Configuration Manager provides several built-in reports and dashboards. Use these to identify problems and trends before they become problems for server or client operations.

Configuration Manager includes several features that provide near real-time service. If these features are critical to meet your business requirements, plan and configure your sites and hierarchies for high availability. For example:

- Client notification actions, such as restart, start Windows Defender scans, or remote desktop.
- State-based messages for monitoring features such as software updates and endpoint protection.
- Scripts, starting in version 1706
- CMPivot, starting in version 1806

Other features of Configuration Manager don't provide real-time service. These features include, but aren't limited to, client settings, hardware and software inventory, software deployments, and compliance settings. Expect them to operate with some data latency. It's unusual for most scenarios that involve a temporary interruption of service to become a critical problem. To minimize downtime, maintain autonomy of operations, and provide a high level of service, configure your sites and hierarchies with high availability in mind.

For example, Configuration Manager clients typically operate autonomously by using known schedules and configurations for operations, and schedules to submit data to the site for processing.

- When clients can't contact the site, they cache data to be submitted until they can contact the site.
- Clients that can't contact the site continue to operate. They use the last known schedules and cached information, until they can contact the site and receive new policies. For example, a client may keep a

previously downloaded application that they must run or install.

- The site monitors its site systems and clients for periodic status updates. It can generate alerts when these components fail to register.
- Built-in reports provide insight to ongoing operations, historical operations, and current trends. Configuration Manager also supports state-based messages that provide near real-time information for ongoing operations.

High availability for sites and hierarchies

Use a site server in passive mode

Starting with version 1806, install an additional site server in *passive* mode for a standalone primary site. The site server in passive mode is in addition to your existing site server in *active* mode. A site server in passive mode is available for immediate use, when needed. For more information, see Site server high availability.

Use a remote content library

Starting with version 1806, move the site's content library to a remote location that provides highly available storage. This feature is a requirement for site server high availability. For more information, see The content library.

Centralize content sources

All software content in Configuration Manager requires a package source location on the network. Use centralized, highly available storage to host a common package source location for all content.

Use a SQL Server Always On availability group to host the site database

Host the site database at primary sites and the central administration site on SQL Server Always On availability groups. For more information, see SQL Server Always On for a highly available site database.

Use a SQL Server cluster to host the site database

When you use a SQL Server cluster for the database at a central administration site or primary site, you use the fail-over support built into SQL Server.

Secondary sites can't use a SQL Server cluster, and don't support backup or restoration of their site database. Recover a secondary site by reinstalling the secondary site from its parent primary site.

Deploy a hierarchy of sites with a central administration site, and one or more child primary sites

This configuration can provide fault tolerance when your sites manage overlapping segments of your network. It also offers an additional recovery option to use the information in the shared database available at another site, to rebuild the site database at the recovered site. Use this option to replace a failed or unavailable backup of the failed site's database.

Create regular backups at central administration sites and primary sites

When you create and test a regular site backup, this makes sure that you have the data necessary to recover a site. You also practice recovering a site in the minimal amount of time.

Install multiple instances of site system roles

When you install multiple instances of critical site system roles, you provide redundant points of contact for clients. For example, multiple management points and distribution points provide redundant service in the event that a specific server is offline.

Install multiple instances of the SMS Provider at a site

The SMS Provider provides the point of administrative contact for one or more Configuration Manager consoles. To provide redundancy for contact points to administer your site and hierarchy, install multiple SMS Providers.

High availability for site system roles

At each site, you deploy site system roles to provide the services that you want clients to use at that site. The site database contains the configuration information for the site and for all clients. Use one or more of the available options to provide for high availability of the site database, and the recovery of the site and site database if needed.

Redundancy for important site system roles

- Application catalog web service point
- Application catalog website point
- Distribution point
- Management point
- Software update point
- State migration point

To provide redundancy for reporting on sites and clients, install multiple instances of the reporting services point.

For failover support with the software update point, use Windows PowerShell to install this role on a Windows network load balancing (NLB) cluster.

Built-in site backup

Configuration Manager includes a built-in backup task to help you back up your site and critical information on a regular schedule. Additionally, the Configuration Manager setup wizard supports site restoration actions to help you restore a site to operations.

Publishing to Active Directory Domain Services and DNS

Configure each site to publish data about the site to Active Directory Domain Services and DNS. This publishing enables clients to identify the most accessible server on the network. Clients also use it to identify when new site system servers are available to provide important services, such as management points.

SMS Provider and Configuration Manager console

Configuration Manager supports installing multiple SMS Providers on separate servers as multiple access points for the console. If one SMS Provider server is offline, you can still view and manage sites and clients.

When a Configuration Manager console connects to a site, it connects to an instance of the SMS Provider at that site. The instance of the SMS Provider is randomly selected. If the selected SMS Provider isn't available, you have the following options:

- Reconnect the console to the site. Each new connection request is randomly assigned an instance of the SMS Provider. It's possible that the new connection is assigned an available instance.
- Connect the console to a different Configuration Manager site and manage the configuration from that connection. This option introduces a slight delay of configuration changes of no more than a few minutes. After the SMS Provider for the site is online, reconnect your Configuration Manager console directly to the site that you want to manage.

Install the Configuration Manager console on multiple computers for use by administrators. Each SMS Provider supports connections from more than one console.

Management point

Install multiple management points at each primary site, and enable the sites to publish site data to your Active Directory infrastructure, and to DNS.

Multiple management points help to load-balance the use of any single management point by multiple clients. Also consider installing one or more database replicas for management points. This configuration decreases the processor-intensive operations of the management point. It also increases the availability of this critical site system

role.

Secondary sites only support installation of one management point, which must be located on the secondary site server. Management points at secondary sites aren't considered to have a highly available configuration.

> **NOTE**
>
> Devices managed by on-premises mobile device management connect to only one management point at a primary site. The management point is assigned by Configuration Manager to the mobile device during enrollment and then doesn't change. When you install multiple management points and enable more than one for mobile devices, the management point that's assigned to a mobile device client is non-deterministic.
>
> If the management point that a mobile device client uses becomes unavailable, you must resolve the problem with that management point or wipe the mobile device and re-enroll the mobile device so that it can be assigned to an operational management point that is enabled for mobile devices.

Distribution point

Install multiple distribution points, and deploy content to multiple distribution points. Add more than one distribution point per boundary group to make sure clients get several options in their content request. Configure boundary group relationships so that they have a predicable fallback behavior to another boundary group or cloud distribution point. For more information, see Configure boundary groups.

Application catalog web service point and application catalog website point

> **IMPORTANT**
>
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features

Install more than one instance of each site system role. For best performance, deploy one of each on the same site system server.

Each application catalog site system role provides the same information as other instances of that role regardless of its location in the hierarchy. When a client makes a request for the application catalog, and you've configured clients to automatically detect the default application catalog website point, the client is directed to an available instance. Clients prefer local application catalog instances, based on the current network location of the client.

For more information about this client setting and how automatic detection works, see the Computer Agent client settings.

High availability for clients

Client operations are autonomous

Configuration Manager client autonomy includes the following behaviors:

- Clients don't require continuous contact with any specific site system servers. They use known configurations to perform preconfigured actions on a schedule.
- Clients can use any available instance of a site system role that provides services to clients. They attempt to contact known servers until they locate an available server.

- Clients can run inventory, software deployments, and similar scheduled actions independent of direct contact with site system servers.
- Clients that are configured to use a fallback status point can submit details to the fallback status point when they can't communicate with a management point.

Clients can repair themselves

Clients automatically remediate most typical issues without direct administrative intervention.

- Periodically, clients self-evaluate their status. They take action to remediate typical problems by using a local cache of remediation steps and source files for repairs.
- When a client fails to submit status information to its site, the site can generate an alert. Administrative users that receive these alerts can take immediate action to restore the normal operation of the client.

Clients cache information to use in the future

When a client communicates with a management point, the client can obtain and cache the following information:

- Client settings
- Client schedules
- Information about software deployments and a download of the software the client is scheduled to install, when the deployment is configured for this action.

When a client can't contact a management point, the clients locally cache the status, state, and client information they report to the site. The client transfers this data after it establishes contact with a management point.

Client can submit status to a fallback status point

When you configure a client to use a fallback status point, you provide an additional point of contact for the client to submit important details about its operation. Clients that are configured to use a fallback status point continue to send status about their operations to that site system role even when the client can't communicate with a management point.

Central management of client data and client identity

The site database, rather than the individual client, retains important information about each client's identity, and associates that data to a specific computer, or user.

- The client source files on a computer can be uninstalled and reinstalled without affecting the historical records for the computer where the client is installed.
- Failure of a client computer doesn't affect the integrity of the information that's stored in the database. This information can remain available for reporting.

Options for sites and site system roles that aren't highly available

Several site systems don't support multiple instances at a site or in the hierarchy. This information can help you prepare for these site systems going offline.

Site server (site)

> **NOTE**
> This section only applies to Configuration Manager versions 1802 and earlier. Starting with version 1806, Configuration Manager provides a high availability option for the site server. For more information, see Site server high availability.

Configuration Manager doesn't support the installation of the site server for each site on a Windows Server cluster or NLB cluster.

Starting in version 1810, the Configuration Manager setup process no longer blocks installation of the site server role on a computer with the Windows role for Failover Clustering. SQL Always On requires this role, so previously you couldn't colocate the site database on the site server. With this change, you can create a highly available site with fewer servers by using SQL Always On and a site server in passive mode.

The following information can help you prepare for when a site server fails or isn't operational:

- Use the built-in backup task to regularly create a backup of the site. In a test environment, regularly practice restoring sites from a backup.
- Deploy multiple Configuration Manager primary sites in a hierarchy with a central administration site to create redundancy. If you experience a site failure, consider using Windows group policy or logon scripts to reassign clients to a functional site.
- If you have a hierarchy with a central administration site, you can recover the central administration site or a child primary site by using the option to recover a site database from another site in your hierarchy.
- Secondary sites can't be restored, and must be reinstalled.

Asset intelligence synchronization point (hierarchy)

This site system role isn't considered mission critical and provides optional functionality in Configuration Manager. If this site system goes offline, use one of the following options:

- Resolve the reason for the site system to be offline.
- Uninstall the role from the current server, and install the role on a new server.

Endpoint protection point (hierarchy)

This site system role isn't considered mission critical and provides optional functionality in Configuration Manager. If this site system goes offline, use one of the following options:

- Resolve the reason for the site system to be offline.
- Uninstall the role from the current server, and install the role on a new server.

Enrollment point (site)

This site system role isn't considered mission critical and provides optional functionality in Configuration Manager. If this site system goes offline, use one of the following options:

- Resolve the reason for the site system to be offline.
- Uninstall the role from the current server, and install the role on a new server.

Enrollment proxy point (site)

This site system role isn't considered mission critical and provides optional functionality in Configuration Manager. However, you can install multiple instances of this site system role at a site, and at multiple sites in the hierarchy. If this site system goes offline, use one of the following options:

- Resolve the reason for the site system to be offline.
- Uninstall the role from the current server, and install the role on a new server.

When you have more than one enrollment proxy server in a site, use a DNS alias for the server name. When you use this configuration, DNS round robin provides some fault tolerance and load balancing for when users enroll their mobile devices.

Fallback status point (site or hierarchy)

This site system role isn't considered mission critical and provides optional functionality in Configuration Manager. If this site system goes offline, use one of the following options:

- Resolve the reason for the site system to be offline.
- Uninstall the role from the current server, and install the role on a new server. Because clients are assigned the fallback status point during client installation, you need to modify existing clients to use the new site system server.

Service connection point (hierarchy)

While this site system role is critical for keeping Configuration Manager current branch up to date, it's generally not used frequently. If this system goes offline, use one of the following options:

- Resolve the reason for the site system to be offline.
- Uninstall the role from the current server, and install the role on a new server.

See also

- Supported configurations
- Recommended hardware
- Supported operating systems for site system servers
- Site and site system prerequisites
- Site failure impacts

Site server high availability in Configuration Manager

5/23/2019 • 14 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Historically, you could add redundancy to most of the roles in Configuration Manager by having multiple instances of these roles in your environment. Except for the site server itself. Starting in Configuration Manager version 1806, high availability for the site server role is a Configuration Manager-based solution to install an additional site server in*passive* mode. Version 1810 adds hierarchy support, so central administration sites and child primary sites can also have an additional site server in passive mode. The site server in passive mode can be on-premises or cloud-based in Azure.

This feature brings the following benefits

- Redundancy and high availability to the site server role
- More easily change the hardware or OS of the site server
- More easily move your site server to Azure IaaS

The site server in passive mode is in addition to your existing site server that is in *active* mode. A site server in passive mode is available for immediate use, when needed. Include this additional site server as part of your overall design for making the Configuration Manager service highly available.

A site server in passive mode:

- Uses the same site database as your site server in active mode.
- Doesn't write data to the site database when it's in passive mode.
- Uses the same content library as your site server in active mode.

To make the site server in passive mode become active, you manually *promote* it. This action switches the site server in active mode to be the site server in passive mode. The site system roles that are available on the original active mode server remain available so long as that computer is accessible. Only the site server role is switched between active and passive modes.

Microsoft Core Services Engineering and Operations used this feature to migrate their central administration site to Microsoft Azure. For more information, see the Microsoft IT Showcase article.

Prerequisites

- The site content library must be on a remote network share. Both site servers need Full Control permissions to the share and its contents. For more information, see Manage content library.
    - The site server computer account needs **Full control** permissions to the network path to which you're moving the content library. This permission applies to both the share and the file system. No components are installed on the remote system.
    - The site server can't have the distribution point role. The distribution point also uses the content library, and this role doesn't support a remote content library. After moving the content library, you can't add the distribution point role to the site server.
- The site server in passive mode can be on-premises or cloud-based in Azure.

> **NOTE**
> A cloud-based site server in passive mode uses Azure infrastructure as a service (IaaS). For more information, see the following articles:
>
> - Azure virtual machines (for cloud-based infrastructure)
> - FAQ for Configuration Manager on Azure

- Both site servers must be joined to the same Active Directory domain.
- In version 1806, the site must be a standalone primary site.
  - Starting in version 1810, Configuration Manager supports site servers in passive mode in a hierarchy. The central administration site and child primary sites can have an additional site server in passive mode.
- Both site servers must use the same site database.
  - In version 1806, the database must be remote from each site server. Starting in version 1810, the Configuration Manager setup process no longer blocks installation of the site server role on a computer with the Windows role for Failover Clustering. SQL Always On requires this role, so previously you couldn't colocate the site database on the site server. With this change, you can create a highly available site with fewer servers by using SQL Always On and a site server in passive mode.
  - The SQL Server that hosts the site database can use a default instance, named instance, SQL Server cluster, or a SQL Server Always On availability group.
  - Both site servers need the **sysadmin** security role on the instance of SQL Server that hosts the site database. The original site server should already have these roles, so add them for the new site server. For example, the following SQL script adds these roles for the new site server **VM2** in the Contoso domain:

    ```
    USE [master]
    GO
    CREATE LOGIN [contoso\vm2$] FROM WINDOWS WITH DEFAULT_DATABASE=[master], DEFAULT_LANGUAGE=
    [us_english]
    GO
    ALTER SERVER ROLE [sysadmin] ADD MEMBER [contoso\vm2$]
    GO
    ```

  - Both site servers need access to the site database on the instance of SQL Server. The original site server should already have this access, so add it for the new site server. For example, the following SQL script adds a login to the **CM_ABC** database for the new site server **VM2** in the Contoso domain:

    ```
    USE [CM_ABC]
    GO
    CREATE USER [contoso\vm2$] FOR LOGIN [contoso\vm2$] WITH DEFAULT_SCHEMA=[dbo]
    GO
    ```

  - The site server in passive mode is configured to use the same site database as the site server in active mode. The site server in passive mode only reads from the database. It doesn't write to the database until after it's promoted to active mode.
- The site server in passive mode:
  - Must meet the prerequisites for installing a primary site. For example, .NET Framework, Remote Differential Compression, and the Windows ADK. For the complete list, see Site and site system

prerequisites.

  - Must have its computer account in the local Administrators group on the site server in active mode.
  - Must install using source files that match the version of the site server in active mode.
  - Can't have a site system role from any site installed on it before you install the site server in passive mode role.

- Both site servers can run different OS or service pack versions, as long as both are supported by Configuration Manager.
- Don't host the service connection point role on either site server configured for high availability. If it's currently on the original site server, remove it, and install it on another site system server. For more information, see About the service connection point.
- Permissions for the site system installation account
  - By default, many customers use the site server's computer account to install new site systems. The requirement is then to add the site server's computer account to the local **Administrators** group on the remote site system. If your environment uses this configuration, make sure to add the computer account of the new site server to this local group on all remote site systems. For example, all remote distribution points.
  - The more secure and recommended configuration is to use a service account for installing the site system. The most secure configuration is to use a local service account. If your environment uses this configuration, no change is needed.

Limitations

- Only a single site server in passive mode is supported at each site.
- In version 1806, a site server in passive mode isn't supported in a hierarchy. A hierarchy includes a central administration site and a child primary site. Only create a site server in passive mode at a standalone primary site.
  - Starting in version 1810, Configuration Manager supports site servers in passive mode in a hierarchy. The central administration site and child primary sites can have an additional site server in passive mode.
- A site server in passive mode isn't supported at a secondary site.

> **NOTE**
> Secondary sites are still supported under a primary site with highly available site servers.

- Promotion of the site server in passive mode to active mode is manual. There's no automatic failover.
- Site system roles can't be installed on the new server before you add the site server in passive mode.

> **NOTE**
> After it installs the site server in passive mode, you can add additional roles as necessary. For example, the SMS Provider, or a management point at a primary site.

- For roles like the reporting point that use a database, host the database on a server that's remote from both site servers.
- When you add the site server in passive mode role, the site doesn't also install the SMS Provider role. Install

at least one additional instance of the provider on another server for high availability. If your design includes this role on your site server, install it on the new site server after you add the site server in passive mode role. For more information, see Plan for the SMS Provider.

- The Configuration Manager console doesn't automatically install on the site server in passive mode.

Add a site server in passive mode

For more information on the general process of adding roles, see Install site system roles.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, select the **Sites** node, and click **Create Site System Server** in the ribbon.
2. On the **General** page of the Create Site System Server Wizard, specify the server to host the site server in passive mode. The server you specify can't host any site system roles before installing a site server in passive mode.
3. On the **System Role Selection** page, select only **Site server in passive mode**.

   > **NOTE**
   >
   > The wizard performs the following initial prerequisite checks on this page:
   >
   > - The selected server isn't a secondary site server
   > - The selected server isn't already a site server in passive mode
   > - The site's content library is in a remote location
   >
   > If these initial prerequisite checks fails, you can't continue past this page of the wizard.

4. On the **Site Server In Passive Mode** page, provide the following information that's used to run setup and install the site server role on the specified server:

   - Choose one of the following options:

     - **Copy installation source files over the network from the site server in active mode**: This option creates a compressed package and sends it to the new site server.
     - **Use the source files at the following location on the site server in passive mode**: For example, a local path to which you already copied the source files. Make sure this content is the same version as the site server in active mode.
     - (*Recommended*) **Use the source files at the following network location**: Specify the path directly to the contents of the **CD.Latest** folder from the site server in active mode. For example, `\\Server\SMS_ABC\CD.Latest` where "*Server*" is the name of the site server in active mode, and "*ABC*" is the site code.

   - Specify the local path at which to install Configuration Manager on the new site server. For example: `C:\Program Files\Configuration Manager`

5. Complete the wizard. Configuration Manager then installs the site server in passive mode on the specified server.

For detailed installation status, in the console go to the **Monitoring** workspace, and select the **Site Server Status** node. The state for the site server in passive mode displays as **Installing**. For more detailed information, select the server and click **Show Status**. This action opens the Site Server Installation Status window. When the process is complete, the state shows **OK** for both servers.

For more information on the setup process, see Flowchart - Set up a site server in passive mode.

After you add a site server in passive mode, see both site servers on the **Nodes** tab in the **Sites** node of the console.

All Configuration Manager site server components are in standby on the site server in passive mode. The Windows services are still running.

Site server promotion

Similarly as with backup and recovery, plan and practice your process to change site servers. Consider the following points in your promotion plan:

- Practice a planned promotion, where both site servers are online. Also practice an unplanned failover, by forcibly disconnecting or shutting down the site server in active mode.
- Determine your operational processes during failover, and what to communicate with other Configuration Manager administrators.
- Before a planned promotion:
  - Check the overall status of the site and site components. Make sure everything is healthy as normal for your environment.
  - Check content status for any packages actively replicating between sites.
  - Check secondary site status and site replication.
  - Don't start any new content distribution jobs or maintenance on child or secondary site servers.

> **NOTE**
> If file or database replication between sites is in progress during failover, the new site server may not receive the replicated content. If this happens, redistribute the software content after the new site server is active. For database replication, you may need to reinitialize a secondary site after failover.

Process to promote the site server in passive mode to active mode

This section describes how to change the site server in passive mode to active mode. To access the site and make this change, you need to be able to access an instance of the SMS Provider. For more information, see Use multiple SMS Providers.

> **IMPORTANT**
> By default, only the original site server has the SMS Provider role. If this server is offline, you can't connect to the site as no provider is available. When you add the site server in passive mode, the SMS Provider isn't automatically added. Add at least one additional SMS Provider role to your site for a highly available service.

> **TIP**
> The Configuration Manager console requests the list of available SMS Providers from WMI on the site server. When you install multiple SMS Providers at a site, the site randomly assigns each new connection request to use an installed SMS Provider. You can't specify the SMS Provider location to use with a specific connection session. If your console is unable to connect to the site because the current site server is offline, specify the other site server in the Site Connection window.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. Select the site, and then switch to the **Nodes** tab. Select the site server in passive mode, and then click **Promote to active** in the ribbon. Click **Yes** to confirm and continue.

2. Refresh the console node. The **Status** column for the server you're promoting displays in the **Nodes** tab as **Promoting**.

3. After the promotion is complete, the **Status** column shows **OK** for both the new site server in active mode, and for the new site server in passive mode. The **Server Name** column for the site now displays the name of the new site server in active mode.

For detailed status, go to the **Monitoring** workspace, and select the **Site Server Status** node. The **Mode** column identifies which server is *Active* or *Passive*. When you promote a server from passive mode to active mode, select the site server that you're promoting to active, and then choose **Show Status** from the ribbon. This action opens the Site Server Promotion Status window that displays additional details about the process.

When a site server in active mode switches over to passive mode, only the site system role is made passive. All other site system roles that are installed on that computer remain active and accessible to clients.

For more information on the *planned* promotion process, see Flowchart - Promote site server (planned).

Unplanned failover

If the current site server in active mode is offline, the site server for promotion tries to contact the current site server in active mode for 30 minutes. If the offline server comes back before this time, it's successfully notified, and the change proceeds gracefully. Otherwise the site server for promotion forcibly updates the site configuration for it to be active. If the offline server comes back after this time, it first checks the current state in the site database. It then proceeds with demoting itself to the site server in passive mode.

During this 30-minute waiting period, the site has no site server in active mode. Clients still communicate with client-facing roles such as management points, software update points, and distribution points. Users can install software that's already deployed. No site administration is possible in this time period. For more information, see Site failure impacts.

If the offline server is damaged such that it can't return, delete this site server from the console. Then create a new site server in passive mode to restore a highly available service.

For more information on the *unplanned* failover process, see Flowchart - Promote site server (unplanned).

Additional tasks after site server promotion

After switching site servers, you don't have to do most of the other tasks as are necessary when recovering a site. For example, you don't need to reset passwords or reconnect your Microsoft Intune subscription.

The following steps may be required if necessary in your environment:

- If you import PKI certificates for distribution points, reimport the certificate for affected servers. For more information, see Regenerate the certificates for distribution points.
- If you integrate Configuration Manager with the Microsoft Store for Business, reconfigure that connection. For more information, see Manage apps from the Microsoft Store for Business.

Daily monitoring

When you have a site server in passive mode, monitor it daily. Make sure its Status remains OK and is ready for use. In the Configuration Manager console, go to the **Monitoring** workspace, and select the **Site Server Status** node. View both site servers and their current status. Also view status in the **Administration** workspace. Expand **Site Configuration**, and select the **Sites** node. Select the site, and then switch to the **Nodes** tab.

Flowchart - Set up a site server in passive mode

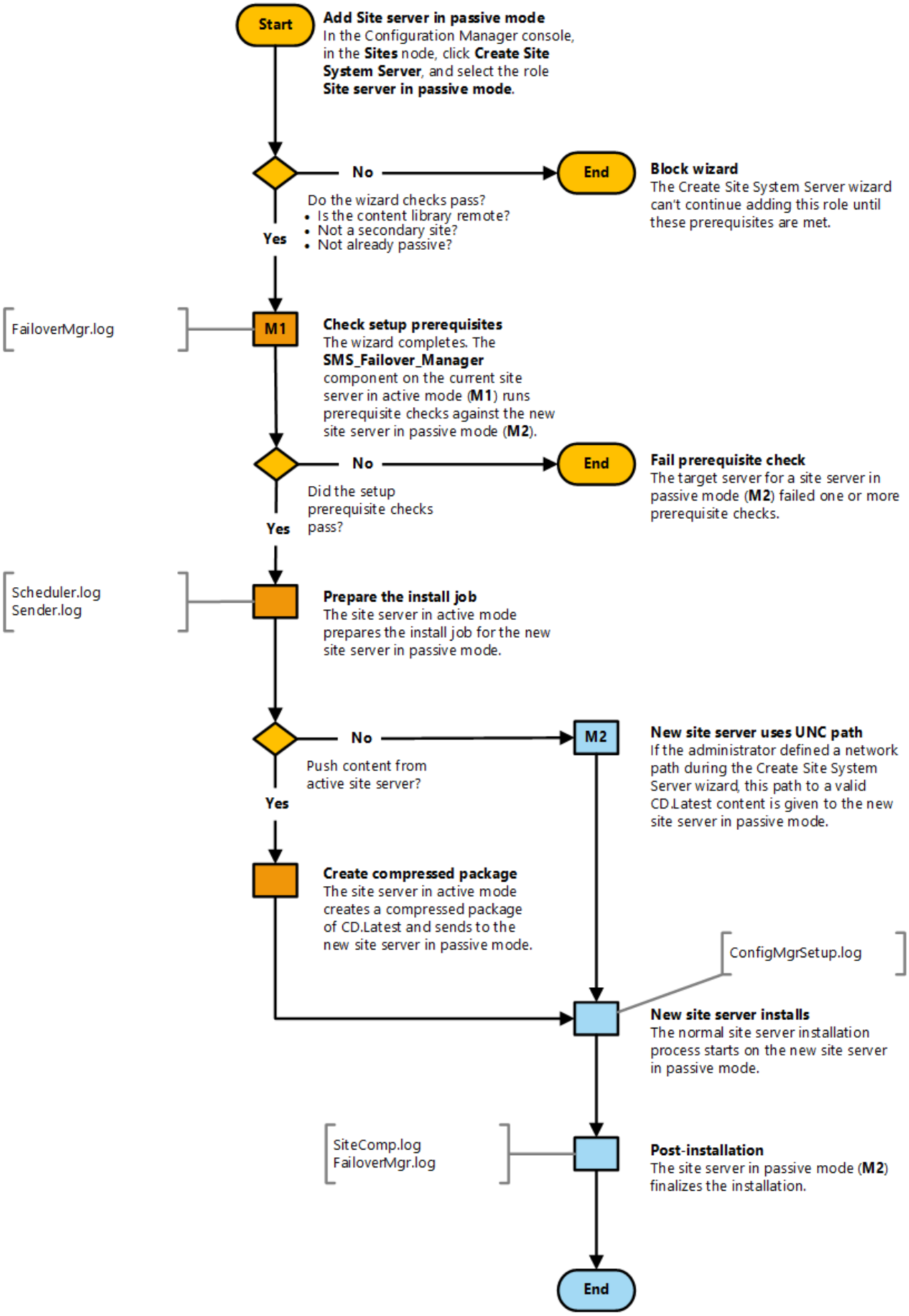
2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This flowchart diagram shows the process by which the site sets up a site server in passive mode. For more information, see the following articles:

- Site server high availability
- Flowchart - Promote site server (planned)
- The content library
- Flowchart - Manage content library

Set up a site server in passive mode



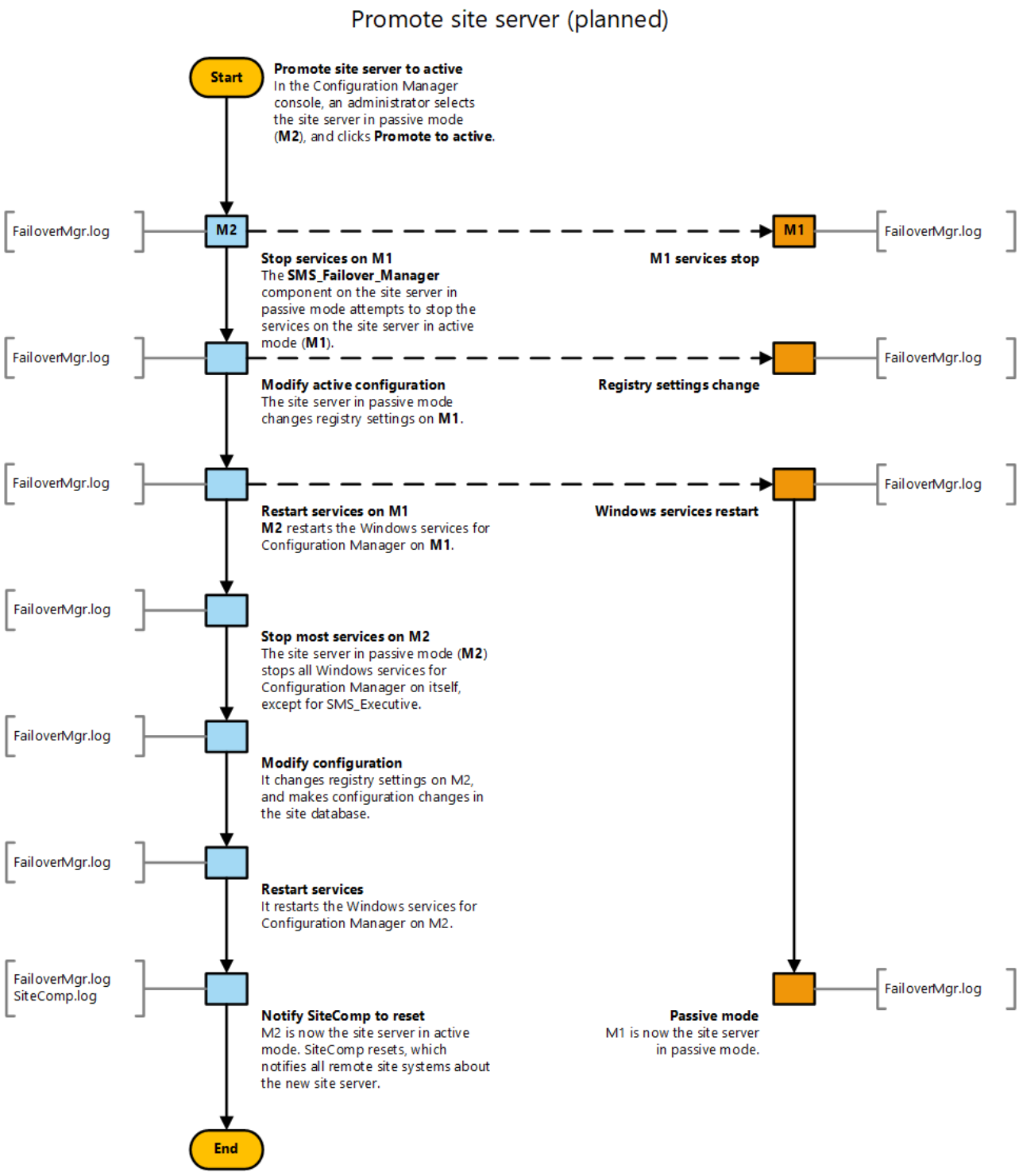
Flowchart - Promote site server (planned)

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This flowchart diagram shows the process by which a site server in passive mode is promoted to the site server in active mode. In this example, the administrator plans for the promotion process. Both servers are online and fully functional. For more information, see the following articles:

- Site server high availability
- Flowchart - Set up a site server in passive mode



Flowchart - Promote site server (unplanned)

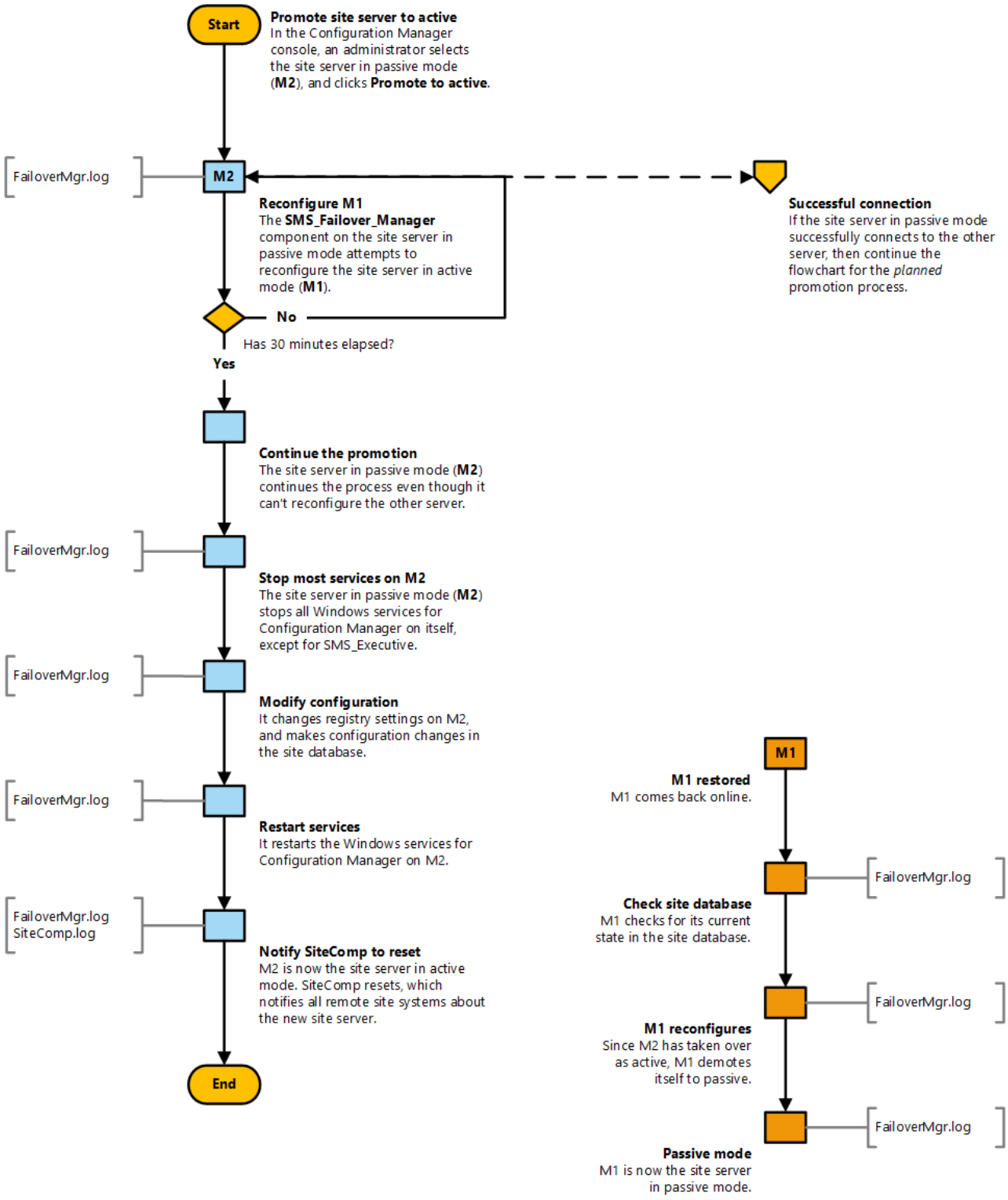
2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This flowchart diagram shows the process by which a site server in passive mode is promoted to the site server in active mode when the current site server in active mode is offline. In this example, the current site server in active mode isn't fully operational, for example it is disconnected from the network or powered off. For more information, see the following articles:

- Site server high availability
- Flowchart - Promote site server (planned)
- Flowchart - Set up a site server in passive mode

Promote site server (unplanned)



Prepare to use SQL Server Always On availability groups with Configuration Manager

9/11/2019 • 14 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use this article to prepare Configuration Manager to use SQL Server Always On availability groups. This feature provides a high availability and disaster recovery solution for the site database.

Configuration Manager supports using availability groups:

- At primary sites and the central administration site.
- On-premises, or in Microsoft Azure.

When you use availability groups in Microsoft Azure, you can further increase availability of your site database by using *Azure Availability Sets*. For more information on Azure Availability Sets, see Manage the availability of virtual machines.

> **IMPORTANT**
> Before you continue, be comfortable with configuring SQL Server and SQL Server availability groups. The information that follows references the SQL Server documentation library and procedures.

Supported scenarios

The following scenarios are supported for using availability groups with Configuration Manager. For more information and procedures for each scenario, see Configure availability groups for Configuration Manager.

- Create an availability group for use with Configuration Manager
- Configure a site to use the availability group
- Add or remove synchronous replica members from an availability group that hosts a site database
- Configure or recover a site from an asynchronous commit replicas
- Move a site database out of an availability group to a default or named instance of a standalone SQL Server

Prerequisites

The following prerequisites apply to all scenarios. If additional prerequisites apply to a specific scenario, they're detailed with that scenario.

Configuration Manager accounts and permissions

Installation account

The account you use to run Configuration Manager setup must be:

- A member of the local **Administrators** group on each computer that's a member of the availability group.
- A **sysadmin** on each instance of SQL Server that hosts the site database.

Site server to replica member access

The computer account of the site server must be a member of the local **Administrators** group on each computer that's a member of the availability group.

SQL Server

Version

Each replica in the availability group must run a version of SQL Server that's supported by your version of Configuration Manager. When supported by SQL Server, different nodes of an availability group can run different versions of SQL Server. For more information, see Supported SQL Server versions for Configuration Manager.

Edition

Use an *Enterprise* edition of SQL Server.

Account

Each instance of SQL Server can run under a domain user account (**service account**) or a non-domain account. Each replica in a group can have a different configuration.

- Use an account with the lowest possible permissions. For more information, see Security considerations for a SQL Server installation.
- For more information on configuring service accounts and permissions for SQL Server, see Configure Windows service accounts and permissions.
- To use a non-domain account, you must use certificates. For more information, see Use certificates for a database mirroring endpoint (Transact-SQL).
- For more information, see Create a database mirroring endpoint for Always On availability groups.

Database

Configure the database on a new replica

Configure the database of each replica with the following settings:

- Enable **CLR Integration**:

  ```
  sp_configure 'show advanced options', 1;
  GO
  RECONFIGURE;
  GO
  sp_configure 'clr enabled', 1;
  GO
  RECONFIGURE;
  GO
  ```

  For more information, see CLR integration.

- Set **Max text repl size** to `2147483647`:

  ```
  EXECUTE sp_configure 'max text repl size (B)', 2147483647
  ```

- Set the database owner to the *SA account*. You don't need to enable this account.

- Turn **ON** the **TRUSTWORTHY** setting:

  ```
  ALTER DATABASE [CM_xxx] SET TRUSTWORTHY ON;
  ```

  For more information, see the TRUSTWORTHY database property.

- Enable the **Service Broker**:

  ```
  ALTER DATABASE [CM_xxx] SET ENABLE_BROKER
  ```

> **NOTE**
> You can't enable the Service Broker option on a database that's already part of an availability group. You have to enable that option before adding it to the availability group.

- Configure the Service Broker priority:

```
ALTER DATABASE [CM_xxx] SET HONOR_BROKER_PRIORITY ON;
ALTER DATABASE [CM_xxx] SET ENABLE_BROKER WITH ROLLBACK IMMEDIATE
```

Only make these configurations on a primary replica. To configure a secondary replica, first fail over the primary to the secondary. This action makes the secondary the new primary replica.

Database verification script

Run the following SQL script to verify database configurations for both primary and secondary replicas. Before you can fix an issue on a secondary replica, change that secondary replica to be the primary replica.

```
    SET NOCOUNT ON

    DECLARE @dbname NVARCHAR(128)

    SELECT @dbname = sd.name FROM sys.sysdatabases sd WHERE sd.dbid = DB_ID()

    IF (@dbname = N'master' OR @dbname = N'model' OR @dbname = N'msdb' OR @dbname = N'tempdb' OR @dbname =
N'distribution' ) BEGIN
    RAISERROR(N'ERROR: Script is targetting a system database.  It should be targeting the DB you created
instead.', 0, 1)
    GOTO Branch_Exit;
    END ELSE
    PRINT N'INFO: Targeted database is ' + @dbname + N'.'

    PRINT N'INFO: Running verifications....'

    IF NOT EXISTS (SELECT * FROM sys.configurations c WHERE c.name = 'clr enabled' AND c.value_in_use = 1)
    PRINT N'ERROR: CLR is not enabled!'
    ELSE
    PRINT N'PASS: CLR is enabled.'

    DECLARE @repltable TABLE (
    name nvarchar(max),
    minimum int,
    maximum int,
    config_value int,
    run_value int )

    INSERT INTO @repltable
    EXEC sp_configure 'max text repl size (B)'

    IF NOT EXISTS(SELECT * from @repltable where config_value = 2147483647 and run_value = 2147483647 )
    PRINT N'ERROR: Max text repl size is not correct!'
    ELSE
    PRINT N'PASS: Max text repl size is correct.'

    IF NOT EXISTS (SELECT db.owner_sid FROM sys.databases db WHERE db.database_id = DB_ID() AND db.owner_sid =
0x01)
    PRINT N'ERROR: Database owner is not sa account!'
    ELSE
    PRINT N'PASS: Database owner is sa account.'

    IF NOT EXISTS( SELECT * FROM sys.databases db WHERE db.database_id = DB_ID() AND db.is_trustworthy_on = 1 )
    PRINT N'ERROR: Trustworthy bit is not on!'
    ELSE
    PRINT N'PASS: Trustworthy bit is on.'

    IF NOT EXISTS( SELECT * FROM sys.databases db WHERE db.database_id = DB_ID() AND db.is_broker_enabled = 1 )
    PRINT N'ERROR: Service broker is not enabled!'
    ELSE
    PRINT N'PASS: Service broker is enabled.'

    IF NOT EXISTS( SELECT * FROM sys.databases db WHERE db.database_id = DB_ID() AND
db.is_honor_broker_priority_on = 1 )
    PRINT N'ERROR: Service broker priority is not set!'
    ELSE
    PRINT N'PASS: Service broker priority is set.'

    PRINT N'Done!'

    Branch_Exit:
```

Availability group configurations

Replica members

- The availability group must have one primary replica.

- Use the same number and type of replicas in an availability group that your version of SQL Server supports.
- You can use an asynchronous commit replica to recover your synchronous replica. For more information, see site database recovery options.

> **WARNING**
> Configuration Manager doesn't support *failover* to use the asynchronous commit replica as your site database. For more information, see Failover and failover modes (Always On availability groups).

Configuration Manager doesn't validate the state of the asynchronous commit replica to confirm it's current. Use of an asynchronous commit replica as the site database can put the integrity of your site and data at risk. This replica can be out of sync by design. For more information, see Overview of SQL Server Always On availability groups.

Each replica member must have the following configuration:

- Use the *default instance* or a *named instance*
- The **Connections in Primary Role** setting is **Allow all connections**
- The **Readable Secondary** setting is **Yes**
- Enabled for **Manual Failover**

> **NOTE**
> In version 1902 and earlier, you need to configure all availability groups on the SQL Server for manual failover. This configuration is needed even if it doesn't host the site database.
>
> Starting in version 1906, Configuration Manager supports using the availability group synchronous replicas when set to **Automatic Failover**. Set **Manual Failover** when:
>
> - You run Configuration Manager setup to specify use of the site database in the availability group.
> - You install any update to Configuration Manager. (Not just updates that apply to the site database).

- All members need the same seeding mode. Configuration Manager setup includes a prerequisite check to verify this configuration when creating a database through install or recovery.

> **NOTE**
> When setup creates the database, and you configure **automatic** seeding, the availability group must have permissions to create the database. This requirement applies to both a new database or recovery. For more information, see Automatic seeding for secondary replica.

Replica member location

Either host all replicas in an availability group on-premises, or host them all on Microsoft Azure. A group that includes an on-premises member and a member in Azure isn't supported.

Configuration Manager setup needs to connect to each replica. When you set up an availability group in Azure, and the group is behind an internal or external load balancer, open the following default ports:

- RPC Endpoint Mapper: **TCP 135**
- SQL Server Service Broker: **TCP 4022**
- SQL over TCP: **TCP 1433**

After setup completes, the following ports must stay open for Configuration Manager:

- SQL Server Service Broker: **TCP 4022**
- SQL over TCP: **TCP 1433**

You can use custom ports for these configurations. Use the same custom ports by the endpoint and on all replicas in the availability group.

Listener

The availability group must have at least one *availability group listener*. When you configure Configuration Manager to use the site database in the availability group, it uses the virtual name of this listener. Although an availability group can contain multiple listeners, Configuration Manager can only make use of one. For more information, see Create or configure a SQL Server availability group listener.

File paths

When you run Configuration Manager setup to configure a site to use the database in an availability group, each secondary replica server must have a SQL Server file path that's identical to the file path for the site database files on the current primary replica. If an identical path doesn't exist, setup fails to add the instance for the availability group as the new location of the site database.

The local SQL Server service account must have **Full Control** permission to this folder.

The secondary replica servers only require this file path while you're using Configuration Manager setup to specify the database instance in the availability group. After it completes configuration of the site database in the availability group, you can delete the unused path from secondary replica severs.

For example, consider the following scenario:

- You create an availability group that uses three SQL Servers.
- Your primary replica server is a new installation of SQL Server 2014. By default, it stores the database .MDF and .LDF files in `C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA`.
- You upgraded both of your secondary replica servers to SQL Server 2014 from previous versions. With the upgrade, these servers keep the original file path to store database files: `C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA`.
- Before moving the site database to this availability group, on each secondary replica server, create the following file path: `C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA`. This path is a duplicate of the path in use on the primary replica, even if the secondary replicas won't use this file location.
- You then grant the SQL Server service account on each secondary replica full control access to the newly created file location on that server.
- You can now successfully run Configuration Manager setup to configure the site to use the site database in the availability group.

Multi-subnet failover

Starting in version 1906, you can enable the MultiSubnetFailover connection string keyword in SQL Server. You also need to manually add the following value to the Windows Registry on the site server:

```
HKLM:\SOFTWARE\Microsoft\SMS\Identification

MSF Enabled : 1 (DWORD)
```

> **WARNING**
> Use of site server high availability and SQL Server Always On with multi-subnet failover doesn't provide the full capabilities of automatic failover for disaster recovery scenarios.

If you need to create an availability group with a member in a remote location, prioritize based on the lowest network latency. High network latency can cause replication failures.

Limitations and known issues

The following limitations apply to all scenarios.

Unsupported SQL Server options and configurations

- **Basic availability groups**: Introduced with SQL Server 2016 Standard edition, basic availability groups don't support read access to secondary replicas. Configuration requires this access. For more information, see Basic SQL Server availability groups.
- **Failover cluster instance**: Failover cluster instances aren't supported for a replica you use with Configuration Manager. For more information, see SQL Server Always On failover cluster instances.
- **MultiSubnetFailover**: In version 1902 and earlier, it's not supported to use an availability group with Configuration Manager in a multi-subnet configuration. You also can't use the MutliSubnetFailover keyword connection string.

  To support this configuration, update Configuration Manager to version 1906 or later. For more information, see the Multi-subnet failover prerequisite.

SQL Servers that host additional availability groups

When the SQL Server hosts one or more availability groups in addition to the group you use for Configuration Manager, it needs specific settings at the time you run Configuration Manager setup. These settings are also needed to install an update for Configuration Manager. Each replica in each availability group must have the following configurations:

- Manual Failover
- Allow any read-only connection

> **NOTE**
> In version 1902 and earlier, you need to configure all availability groups on the SQL Server for manual failover. This configuration is needed even if it doesn't host the site database.
>
> Starting in version 1906, Configuration Manager supports using the availability group synchronous replicas when set to **Automatic Failover**. Set **Manual Failover** when:
>
> - You run Configuration Manager setup to specify use of the site database in the availability group.
> - You install any update to Configuration Manager. (Not just updates that apply to the site database).

Unsupported database use

Configuration Manager supports only the site database in an availability group

The following databases aren't supported by Configuration Manager in a SQL Server Always On availability group:

- Reporting database
- WSUS database

Pre-existing database

You can't use a new database created on the replica. When you configure an availability group, restore a copy of an existing Configuration Manager database to the primary replica.

Distributed views

In version 1902 and earlier, if you host the site database on a SQL Server Always On availability group, you can't enable distributed views for database replication. To support this configuration, update to version 1906 or later.

Setup errors in ConfigMgrSetup.log

When you run Configuration Manager setup to move a site database to an availability group, it tries to process database roles on the secondary replicas of the availability group. The **ConfigMgrSetup.log** file shows the following error:

```
ERROR: SQL Server error: [25000][3906][Microsoft][SQL Server Native Client 11.0][SQL Server]Failed to update
database "CM_AAA" because the database is read-only. Configuration Manager Setup 1/21/2016 4:54:59 PM 7344
(0x1CB0)
```

These errors are safe to ignore.

Site expansion

If you configure the site database for a standalone primary site to use SQL Always On, you can't expand the site to include a central administration site. If you try this process, it fails. To expand the site, temporarily remove the primary site database from the availability group.

You don't need to make any changes to the configuration when adding a secondary site.

Changes for site backup

Backup database files

When a site database uses an availability group, run the built-in **Backup Site server** maintenance task to back up common Configuration Manager settings and files. Don't use the .MDF or .LDF files created by that backup. Instead, make direct backups of these database files by using SQL Server.

Transaction log

Set the recovery model of the site database to **Full**. This configuration is a requirement for Configuration Manager use in an availability group. Plan to monitor and maintain the size of the site database transaction log. In the full recovery model, the transactions aren't hardened until it makes a full backup of the database or transaction log. For more information, see Back up and restore of SQL Server databases.

Changes for site recovery

If at least one node of the availability group is still functional, use the site recovery option to **Skip database recovery (Use this option if the site database was unaffected)**.

Starting in version 1906, site recovery can recreate the database on a SQL Always On group. This process works with both manual and automatic seeding.

In version 1902 or earlier, when you lose all nodes of an availability group, before you can recover the site, first recreate the availability group. Configuration Manager can't rebuild or restore the availability node. Recreate the group, restore the backup, and reconfigure SQL. Then use the site recovery option to **Skip database recovery (Use this option if the site database was unaffected)**.

For more information, see Backup and recovery.

Changes for reporting

Install the reporting service point

The reporting services point doesn't support using the listener virtual name of the availability group. It also doesn't

support hosting its database in a SQL Server Always On availability group.

- By default, the reporting services point installation sets the **Site database server name** to the virtual name that's specified as the listener. Change this setting to specify a computer name and instance of a replica in the availability group.
- To offload reporting and to increase availability when a replica node is offline, consider installing additional reporting services points on each replica node. Then configure each reporting services point to use its own computer name. When you install a reporting service point on each replica of the availability group, reporting can always connect to an active reporting point server.

Switch the reporting services point used by the console

1. In the Configuration Manager console, go to the **Monitoring** workspace, expand **Reporting**, and select the **Reports** node.
2. In the ribbon, select **Report Options**.
3. In the Report Options dialog box, select the reporting services point you want to use.

Next steps

This article describes the prerequisites, limitations, and changes to common tasks that Configuration Manager requires when you use availability groups. For procedures to set up and configure your site to use availability groups, see Configure availability groups.

Configure SQL Server Always On availability groups for Configuration Manager

9/5/2019 • 7 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the information in this article to configure and manage the availability groups you use with Configuration Manager.

Before you start:

- Be familiar with the information from Prepare to use SQL Server Always On availability groups with Configuration Manager.
- Be familiar with SQL Server documentation that covers the use of availability groups and related procedures. That information is required to complete the following scenarios.

Create and configure an availability group

Use the following procedure to create an availability group and then move a copy of the site database to that availability group.

1. Use the following command to stop the Configuration Manager site:

   ```
   preinst.exe /stopsite
   ```

   For more information, see Hierarchy maintenance tool.

2. Change the backup model for the site database from **SIMPLE** to **FULL**:

   ```
   ALTER DATABASE [CM_xxx] SET RECOVERY FULL;
   ```

   Availability groups only support the FULL backup model. For more information, see View or change the recovery model of a database.

3. Use SQL Server to create a full backup of your site database. Choose one of the following options:

   - **Will be member of your availability group**: If you use this server as the initial primary replica member of the availability group, you don't need to restore a copy of the site database to this server or another in the group. The database is already in place on the primary replica. SQL Server replicates the database to the secondary replicas during a later step.
   - **Will not be a member of the availability group**: Restore a copy of the site database to the server that will host the primary replica of the group.

   For more information, see the following articles in the SQL Server documentation:

   - Create a full database backup
   - Restore a database backup using SSMS

> **NOTE**
> If you plan to move from an availability group to standalone on an existing replica, first remove the database from the availability group.

4. On the server that will host the initial primary replica of the group, use the New availability group wizard to create the availability group. In the wizard:
   - On the **Select Database** page, select the database for your Configuration Manager site.
   - On the **Specify Replicas** page, configure:
     - **Replicas:** Specify the servers that will host secondary replicas.
     - **Listener:** Specify the **Listener DNS Name** as a full DNS name, for example `<listener_server>.fabrikam.com`. When you configure Configuration Manager to use the database in the availability group, it uses this name.
   - On the **Select Initial Data Synchronization** page, select **Full**. After the wizard creates the availability group, the wizard backs up the primary database and transaction log. Then the wizard restores them on each server that hosts a secondary replica.

     > **NOTE**
     > If you don't use this step, restore a copy of the site database to each server that hosts a secondary replica. Then manually join that database to the group.

5. Check the configuration on each replica:
   a. Make sure the computer account of the site server is a member of the local **Administrators** group on each computer that's a member of the availability group.
   b. Run the verification script to confirm that the site database on each replica is correctly configured.
   c. If it's necessary to set configurations on secondary replicas, before you continue, manually fail over the primary replica to the secondary replica. You can only configure the database of a primary replica. For more information, see Perform a planned manual failover of an availability group in the SQL Server documentation.
6. After all replicas meet the requirements, the availability group is ready to be used with Configuration Manager.

Configure a site to use the availability group

After you create and configure the availability group, use Configuration Manager site maintenance to configure the site to use the database that the availability group hosts.

It's not supported to install a new site with its database in an availability group. For example, if you use baseline media, install the site using a single instance of SQL Server. After the site installs, then move the site database to the availability group.

1. Run **Configuration Manager Setup**: `\BIN\X64\setup.exe` from the Configuration Manager site installation folder.
2. On the **Getting Started** page, select **Perform site maintenance or reset this site**, and then select **Next**.
3. Select **Modify SQL Server configuration**, and then select **Next**.

4. Reconfigure the following settings for the site database:

   - **SQL Server name**: Enter the virtual name for the availability group *listener*. You configured the listener when you created the availability group. The virtual name should be a full DNS name, like `<Listener_Server>.fabrikam.com`.
   - **Instance:** To specify the default instance for the *listener* of the availability group, this value must be blank. If the current site database runs on a named instance, clear the current named instance.
   - **Database:** Leave the name as it appears. This name is the current site database.

5. After you provide the information for the new database location, complete setup with your normal process and configurations.

Synchronous replica members

When your site database is hosted in an availability group, use the following procedures to add or remove synchronous replica members. For more information about the supported type and number of replicas, see Availability group configurations.

Add a new synchronous replica member

Starting in version 1906, run Configuration Manager setup to add a new synchronous replica member.

1. Add a secondary replica using the SQL Server procedures.

   a. Add a secondary replica to an Always On Availability Group.

   b. Watch the status in SQL Management Studio. Wait for the availability group to return to full health.

2. Run Configuration Manager setup, and select the option to modify the site.

3. Specify the availability group listener name as the database name. If the listener uses a non-standard network port, specify that as well. This action causes setup to make sure each node is appropriately configured. It also starts a database recovery process.

Configuration Manager setup uses the SQL database move operation, and makes sure the nodes are correctly configured.

For more information on how to do this process manually in version 1902 or earlier, see ConfigMgr 1702: Adding a new node (Secondary Replica) to an existing SQL AO AG.

Remove a replica member

Starting in version 1906, you can use Configuration Manager setup to remove a replica member. Use the same process to Add a new synchronous replica member.

For more information on how to do this process manually in version 1902 or earlier, see Remove a secondary replica from an availability group.

Asynchronous replicas

You can use an asynchronous replica in the availability group that you use with Configuration Manager. You don't need to run the configuration scripts required to configure a synchronous replica, because an asynchronous replica isn't supported for the site database.

Configure an asynchronous commit replica

For more information, see Add a secondary replica to an availability group.

Use the asynchronous replica to recover your site

Use the asynchronous replica to recover your site database.

1. Stop the active primary site to prevent additional writes to the site database. To stop the site, use the Hierarchy maintenance tool: `preinst.exe /stopsite`
2. After you stop the site, use the asynchronous replica instead of a manually recovered database.

Stop using an availability group

Use the following procedure when you no longer want to host your site database in an availability group. With this process, you'll move the site database back to a single instance of SQL Server.

1. Stop the Configuration Manager site by using the following command: `preinst.exe /stopsite`. For more information, see Hierarchy maintenance tool.
2. Use SQL Server to create a full backup of your site database from the primary replica. For more information, see Create a full database backup.
3. Use SQL Server to restore the site database backup to the server that will host the site database. For more information, see Restore a database backup using SSMS.

   > **NOTE**
   > If the primary replica server for the availability group will host the single instance of the site database, skip this step.

4. On the server that will host the site database, change the backup model for the site database from **FULL** to **SIMPLE**. For more information, see View or change the recovery model of a database.
5. Run **Configuration Manager Setup**: `\BIN\X64\setup.exe` from the Configuration Manager site installation folder.
6. On the **Getting Started** page, select **Perform site maintenance or reset this site**, and then select **Next**.
7. Select **Modify SQL Server configuration**, and then select **Next**.
8. Reconfigure the following settings for the site database:
   - **SQL Server name:** Enter the name of the server that now hosts the site database.
   - **Instance:** Specify the named instance that hosts the site database. If the database is on the default instance, leave this field blank.
   - **Database:** Leave the name as it appears. This name is the current site database.
9. After you provide the information for the new database location, complete setup with your normal process and configurations. When setup completes, the site restarts, and begins to use the new database location.
10. To clean up the servers that were members of the availability group, follow the guidance in Remove an availability group.

Use a SQL Server cluster for the site database

3/26/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can use a SQL Server Failover cluster to host the Configuration Manager site database. A cluster provides failover support and improves the reliability of the site database. However, it doesn't provide additional processing or load-balancing benefits. Additionally, a SQL Server Failover cluster uses shared storage and introduces a single point of failure. Degradation in performance can occur, because the site server must find the active node of the SQL Server cluster before it connects to the site database.

> **IMPORTANT**
> Successful set up of SQL Server clusters relies on documentation and procedures provided in the SQL Server documentation library.

Before you install Configuration Manager, prepare the SQL Server cluster to support Configuration Manager. For more information, see Prepare a clustered SQL Server instance.

During Configuration Manager setup, the Windows Volume Shadow Copy Service writer installs on each physical computer node of the Microsoft Windows Server cluster. This service supports the **Backup Site Server** maintenance task.

After the site installs, Configuration Manager checks for changes to the cluster node each hour. Configuration Manager automatically manages any changes that are found that affect its component installs. For example, a node failover, or the addition of a new node to the SQL Server cluster.

Supported options

The following options are supported for SQL Server failover clusters used as the site database:

- A single instance cluster
- Multiple instance configurations
- Multiple active nodes
- Both a named or a default instance

Prerequisites

Be aware of the following prerequisites:

- The site database must be remote from the site server. The cluster can't include the site system server.

  > **NOTE**
  > Starting in version 1810, the Configuration Manager setup process no longer blocks installation of the site server role on a computer with the Windows role for Failover Clustering. Previously you couldn't colocate the site database on the site server. With this change, you can create a highly available site with fewer servers by using a SQL cluster and a site server in passive mode. For more information, see High availability options.

- Add the computer account of the site server to the local **Administrators** group of each server in the cluster.
- To support Kerberos authentication, enable the **TCP/IP** network communication protocol for the network connection of each SQL Server cluster node. The **Named pipes** protocol isn't required, but can be used to troubleshoot Kerberos authentication issues. The network protocol settings are configured in **SQL Server Configuration Manager**, under **SQL Server Network Configuration**.
- If you use a public key infrastructure (PKI), see PKI certificate requirements. There are specific certificate requirements when you use a SQL Server cluster for the site database.

Limitations

Consider the following limitations:

Installation and configuration

- Secondary sites can't use a SQL Server cluster.
- When you specify a SQL Server cluster, the option to specify non-default file locations for the site database isn't available.

SMS Provider

You can't install an instance of the SMS Provider on a SQL Server cluster. It's also not supported on a computer that runs as a clustered SQL Server node.

Data replication options

If you use **Distributed Views**, you can't use a SQL Server cluster to host the site database.

Backup and recovery

Configuration Manager doesn't support Data Protection Manager (DPM) backup for a SQL Server cluster that uses a named instance. It does support DPM backup on a SQL Server cluster that uses the default instance of SQL Server.

Prepare a clustered SQL Server instance

Here are the main tasks to complete to prepare your site database:

- Create the virtual SQL Server cluster to host the site database on an existing Windows Server cluster environment. For specific steps to install and set up a SQL Server cluster, see the documentation specific to your version of SQL Server. For more information, see Create a new SQL Server Failover Cluster.
- On each computer in the SQL Server cluster, place a file in the root folder of each drive where you don't want Configuration Manager to install site components. Name the file `NO_SMS_ON_DRIVE.SMS`. By default, Configuration Manager installs some components on each physical node, to support operations such as backup.
- Add the computer account of the site server to the local **Administrators** group of each Windows Server cluster node computer.
- In the virtual SQL Server instance, assign the **sysadmin** SQL Server role to the user account that runs Configuration Manager setup.

To install a new site using a clustered SQL Server

To install a site that uses a clustered site database, run Configuration Manager setup following your normal process for installing a site, with the following alteration:

- On the **Database Information** page, specify the name of the virtual SQL Server cluster instance that will host the site database. The virtual instance replaces the name of the computer that runs SQL Server.

IMPORTANT

When you enter the name of the virtual SQL Server cluster instance, don't enter the virtual Windows Server name created by the Windows Server cluster. If you use the virtual Windows Server name, the site database installs on the local hard drive of the active Windows Server cluster node. This prevents successful failover if that node fails.

Custom locations for System Center Configuration Manager site database files

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

System Center Configuration Manager supports custom locations for SQL Server database files.

> **NOTE**
> The option to specify non-default file locations is not available when you use a SQL Server cluster.

During setup of a new primary site or central administration site, you can:

- **Specify non-default file locations for the site database**: Configuration Manager setup then creates the site database using these locations.
- **Specify the use of a pre-created SQL Server database that uses custom file locations**: Configuration Manager setup then uses that pre-created database and its pre-configured file locations.

After setup, you can change the location of the site database files. This requires you to stop the site and edit the file location in SQL Server:

- On the Configuration Manager site server, stop the **SMS_Executive** service.
- Use the documentation for your version of SQL Server to guide you on how to move a user database. For example, if you use SQL Server 2014, see Move User Databases on TechNet.
- After you complete the database file move, restart the **SMS_Executive** service on the Configuration Manager site server.

Configure role-based administration for Configuration Manager

7/26/2019 • 16 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

In Configuration Manager, role-based administration combines security roles, security scopes, and assigned collections to define the administrative scope for each administrative user. An administrative scope includes the objects that an administrative user can view in the Configuration Manager console and the tasks related to those objects that the administrative user has permission to perform. Role-based administration configurations are applied at each site in a hierarchy.

If you're not yet familiar with concepts for role-based administration, see Fundamentals of role-based administration.

The information in the following procedures can help you create and configure role-based administration and related security settings:

- Create custom security roles
- Configure security roles
- Configure security scopes for an object
- Configure collections to manage security
- Create a new administrative user
- Modify the administrative scope of an administrative user

Create custom security roles

Configuration Manager provides several built-in security roles. If you require additional security roles, you can create a custom security role by creating a copy of an existing security role, and then modifying the copy. You might create a custom security role to grant administrative users the additional security permissions they require that aren't included in a currently assigned security role. By using a custom security role, you can grant them only the permissions they require, and avoid assigning a security role that grants more permissions than they require.

Use the following procedure to create a new security role by using an existing security role as a template.

To create custom security roles

1. In the Configuration Manager console, go to **Administration**.
2. In the **Administration** workspace, expand **Security**, and then choose **Security Roles**.

   Use one of the following processes to create the new security role:

   - To create a new custom security role, perform the following actions:

     a. Select an existing security role to use as the source for the new security role.

     b. On the **Home** tab, in the **Security Role** group, choose **Copy**. This action creates a copy of the source security role.

     c. In the Copy Security Role wizard, specify a **Name** for the new custom security role.

     d. In **Security operation assignments**, expand each **Security Operations** node to display the available actions.

e. To change the setting for a security operation, choose the down arrow in the **Value** column, and choose either **Yes** or **No**.

   Caution

   When you configure a custom security role, ensure that you don't grant permissions that aren't required by administrative users that are associated with the new security role. For example, the **Modify** value for the **Security Roles** security operation grants administrative users permission to edit any accessible security role – even if they aren't associated with that security role.

f. After you configure the permissions, choose **OK** to save the new security role.

- To import a security role that was exported from another Configuration Manager hierarchy, perform the following actions:

  a. On the **Home** tab, in the **Create** group, choose **Import Security Role**.

  b. Specify the .xml file that contains the security role configuration that you want to import. Choose **Open** to complete the procedure and save the security role.

  > **NOTE**
  > After you import a security role, you can edit the security role properties to change the object permissions that are associated with the security role.

Configure security roles

The groups of security permissions that are defined for a security role are called security operation assignments. Security operation assignments represent a combination of object types and actions that are available for each object type. You can modify which security operations are available for any custom security role, but you can't modify the built-in security roles that Configuration Manager provides.

Use the following procedure to modify the security operations for a security role.

To modify security roles

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Security**, and then choose **Security Roles**.
3. Select the custom security role that you want to modify.
4. On the **Home** tab, in the **Properties** group, choose **Properties**.
5. Choose the **Permissions** tab.
6. In **Security operation assignments**, expand each **Security Operations** node to display the available actions.
7. To change the setting for a security operation, choose the down arrow in the **Value** column, and then choose either **Yes** or **No**.

   Caution

   When you configure a custom security role, ensure that you don't grant permissions that aren't required by administrative users that are associated with the new security role. For example, the **Modify** value for the **Security Roles** security operation grants administrative users permission to edit any accessible security role – even if they aren't associated with that security role.

8. When you've finished configuring security operation assignments, choose **OK** to save the new security role.

Configure security scopes for an object

You manage the association of a security scope for an object from the object–not from the security scope. The only direct configurations that security scopes support are changes to its name and description. To change the name and description of a security scope when you view the security scope properties, you must have the **Modify** permission for the **Security Scopes** securable object.

When you create a new object in Configuration Manager, it's associated with each security scope that's associated with the security roles of the account used to create the object. This behavior occurs when those security roles provide the **Create** permission or **Set Security Scope** permission. You can change the security scopes for the object after you create it.

As an example, you're assigned a security role that grants you permission to create a new boundary group. When you create a new boundary group, you have no option that you can assign specific security scopes to. Instead, the security scopes that are available from the security roles you're associated with are automatically assigned to the new boundary group. After you save the new boundary group, you can edit the security scopes that are associated with the new boundary group.

Use the following procedure to configure the security scopes that are assigned to an object.

To configure security scopes for an object

1. In the Configuration Manager console, select an object that supports being assigned to a security scope.
2. On the **Home** tab, in the **Classify** group, choose **Set Security Scopes**.
3. In the **Set Security Scopes** dialog box, select or clear the security scopes that this object is associated with. Each object that supports security scopes must be assigned to at least one security scope.
4. Choose **OK** to save the assigned security scopes.

> **NOTE**
> When you create a new object, you can assign the object to multiple security scopes. To modify the number of security scopes that are associated with the object, you must change this assignment after the object is created.

To configure security scopes for a folder (starting in version 1906)

1. In the Configuration Manager console, select a folder.
2. On the **Folder** tab in the ribbon, choose **Set Security Scopes**.
   - You can also right-click the folder and choose **Folder** > **Set Security Scopes**.
3. In the **Set Security Scopes** dialog box, select or clear security scopes for the folder. Each folder must be assigned to at least one security scope. All folders are assigned the **Default** security scope until you change it.
4. Choose **OK** to save the assigned security scopes.

> **IMPORTANT**
> Existing security roles will automatically get **Folder Class** permissions added when you install Configuration Manager version 1906. You'll need to add **Folder Class** permissions for any new security roles and verify existing roles have the appropriate permissions for your environment.

Configure collections to manage security

There are no procedures to configure collections for role-based administration. Collections don't have a role-

based administration configuration. Instead, you assign collections to an administrative user when you configure the administrative user. The collection security operations that are enabled in the user-assigned security roles determine the permissions that an administrative user has for collections and collection resources (collection members).

When an administrative user has permissions to a collection, they also have permissions to collections that are limited to that collection. As an example, your organization uses a collection named All Desktops. There's also a collection named All North America Desktops that's limited to the All Desktops collection. If an administrative user has permissions to All Desktops, they also have those same permissions to the All North America Desktops collection.

Additionally, an administrative user can't use the **Delete** or **Modify** permission on a collection that's directly assigned to them. But, they can use these permissions on the collections that are limited to that collection. In the previous example, the administrative user can delete or modify the All North America Desktops collection, but they can't delete or modify the All Desktops collection.

Create a new administrative user

To grant individuals or members of a security group access to manage Configuration Manager, create an administrative user in Configuration Manager and specify the Windows account of the User or User Group. Each administrative user in Configuration Manager must be assigned at least one security role and one security scope. You can also assign collections to limit the administrative scope of the administrative user.

Use the following procedures to create new administrative users.

To create a new administrative user

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Security**, and then choose **Administrative Users**.
3. On the **Home** tab, in the **Create** group, choose **Add User or Group**.
4. Choose **Browse**, and then select the user account or group to use for this new administrative user.

   > **NOTE**
   > For console-based administration, only domain users or security groups can be specified as an administrative user.

5. For **Associated security roles**, choose **Add** to open a list of the available security roles, check the box for one or more security roles, and then choose **OK**.
6. Choose one of the following two options to define the securable object behavior for the new user:

   - **All instances of the objects that are related to the assigned security roles**: This option associates the administrative user with the **All** security scope, and the **All Systems** and **All Users and User Groups** collections. The security roles that are assigned to the user define access to objects. New objects that this administrative user creates are assigned to the **Default** security scope.
   - **Only the instances of objects that are assigned to the specified security scopes and collections**: By default, this option associates the administrative user with the **Default** security scope, and the **All Systems** and **All Users and User Groups** collections. However, the actual security scopes and collections are limited to those that are associated with the account that you used to create the new administrative user. This option supports the addition or removal of security scopes and collections to customize the administrative scope of the administrative user.

> **IMPORTANT**
> The preceding options associate each assigned security scope and collection to each security role that is assigned to the administrative user. You can use a third option, **Associate assigned security roles with specific security scopes and collections**, to associate individual security roles to specific security scopes and collections. This third option is available after you create the new administrative user, when you modify the administrative user.

7. Depending on your selection in step 6, take the following action:

   - If you selected **All instances of the objects that are related to the assigned security roles**, choose **OK** to complete this procedure.
   - If you selected **Only the instances of objects that are assigned to the specified security scopes and collections**, you can choose **Add** to select additional collections and security scopes. Or select one or more objects in the list, and then choose **Remove** to remove them. Choose **OK** to complete this procedure.

Modify the administrative scope of an administrative user

You can modify the administrative scope of an administrative user by adding or removing security roles, security scopes, and collections that are associated with the user. Each administrative user must be associated with at least one security role and one security scope. You might have to assign one or more collections to the administrative scope of the user. Most security roles interact with collections and don't function correctly without an assigned collection.

When you modify an administrative user, you can change the behavior for how securable objects are associated with the assigned security roles. The three behaviors that you can select are as follows:

- **All instances of the objects that are related to the assigned security roles**: This option associates the administrative user with the **All** scope, and the **All Systems** and **All Users and User Groups** collections. The security roles that are assigned to the user define access to objects.
- **Only the instances of objects that are assigned to the specified security scopes and collections**: This option associates the administrative user to the same security scopes and collections that are associated to the account you use to configure the administrative user. This option supports the addition or removal of security roles and collections to customize the administrative scope of the administrative user.
- **Associate assigned security roles with specific security scopes and collections**: This option lets you create specific associations between individual security roles and specific security scopes and collections for the user.

> **NOTE**
> This option is available only when you modify the properties of an administrative user.

The current configuration for the securable object behavior changes the process that you use to assign additional security roles. Use the following procedures that are based on the different options for securable objects to help you manage an administrative user.

Use the following procedure to view and manage the configuration for securable objects for an administrative user.

To view and manage the securable object behavior for an administrative user

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Security**, and then choose **Administrative Users**.

3. Select the administrative user that you want to modify.
4. On the **Home** tab, in the **Properties** group, choose **Properties**.
5. Choose the **Security Scopes** tab to view the current configuration for securable objects for this administrative user.
6. To modify the securable object behavior, select a new option for securable object behavior. After you change this configuration, see the appropriate procedure for further guidance to configure security scopes and collections, and security roles for this administrative user.
7. Choose **OK** to complete the procedure.

Use the following procedure to modify an administrative user that has the securable object behavior set to **All instances of the objects that are related to the assigned security roles**.

For option: All instances of the objects that are related to the assigned security roles

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Security**, and then choose **Administrative Users**.
3. Select the administrative user that you want to modify.
4. On the **Home** tab, in the **Properties** group, choose **Properties**.
5. Choose the **Security Scopes** tab to confirm that the administrative user is configured for **All instances of the objects that are related to the assigned security roles**.
6. To modify the assigned security roles, choose the **Security Roles** tab.
   - To assign additional security roles to this administrative user, choose **Add**, check the box for each additional security role that you want to assign, and then choose **OK**.
   - To remove security roles, select one or more security roles from the list, and then choose **Remove**.
7. To modify the securable object behavior, choose the **Security Scopes** tab and choose a new option for the securable object behavior. After you change this configuration, see the appropriate procedure for further guidance to configure security scopes and collections, and security roles for this administrative user.

   > **NOTE**
   > When the securable object behavior is set to **All instances of the objects that are related to the assigned security roles**, you can't add or remove specific security scopes and collections.

8. Choose **OK** to complete this procedure.

Use the following procedure to modify an administrative user that has the securable object behavior set to **Only the instances of objects that are assigned to the specified security scopes and collections**.

For option: Only the instances of objects that are assigned to the specified security scopes and collections

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Security**, and then choose **Administrative Users**.
3. Select the administrative user that you want to modify.
4. On the **Home** tab, in the **Properties** group, choose **Properties**.
5. Choose the **Security Scopes** tab to confirm that the user is configured for **Only the instances of objects that are assigned to the specified security scopes and collections**.
6. To modify the assigned security roles, choose the **Security Roles** tab.
   - To assign additional security roles to this user, choose **Add**, check the box for each additional security

role that you want to assign, and then choose **OK**.

- To remove security roles, select one or more security roles from the list, and then choose **Remove**.

7. To modify the security scopes and collections that are associated with security roles, choose the **Security Scopes** tab.

   - To associate new security scopes or collections with all security roles that are assigned to this administrative user, choose **Add** and select one of the four options. If you select **Security Scope** or **Collection**, check the box for one or more objects to complete that selection, and then choose **OK**.
   - To remove a security scope or collection, choose the object, and then choose **Remove**.

8. Choose **OK** to complete this procedure.

Use the following procedure to modify an administrative user that has the securable object behavior set to **Associate assigned security roles with specific security scopes and collections**.

For option: Associate assigned security roles with specific security scopes and collections

1. In the Configuration Manager console, choose **Administration**.
2. In the **Administration** workspace, expand **Security**, and then choose **Administrative Users**.
3. Select the administrative user that you want to modify.
4. On the **Home** tab, in the **Properties** group, choose **Properties**.
5. Choose the **Security Scopes** tab to confirm that the administrative user is configured for **Associate assigned security roles with specific security scopes and collections**.
6. To modify the assigned security roles, choose the **Security Roles** tab.

   - To assign additional security roles to this administrative user, choose **Add**. On the **Add Security Role** dialog box, select one or more available security roles, choose **Add**, and select an object type to associate with the selected security roles. If you select **Security Scope** or **Collection**, check the box for one or more objects to complete that selection, and then choose **OK**.

     > **NOTE**
     > You must configure at least one security scope before the selected security roles can be assigned to the administrative user. When you select multiple security roles, each security scope and collection that you configure is associated with each of the selected security roles.

   - To remove security roles, select one or more security roles from the list, and then choose **Remove**.

7. To modify the security scopes and collections that are associated with a specific security role, choose the **Security Scopes** tab, select the security role, and then choose **Edit**.

   - To associate new objects with this security role, choose **Add**, and select an object type to associate with the selected security roles. If you select **Security Scope** or **Collection**, check the box for one or more objects to complete that selection, and then choose **OK**.

     > **NOTE**
     > You must configure at least one security scope.

   - To remove a security scope or collection that is associated with this security role, select the object, and then choose **Remove**.
   - When you have finished modifying the associated objects, choose **OK**.

8. Choose **OK** to complete this procedure.

Caution

When a security role grants administrative users the collection deployment permission, those administrative users can distribute objects from any security scope for which they have object **read** permissions, even if that security scope is associated with a different security role.

Next steps

Accounts used in Configuration Manager

Configure Azure services for use with Configuration Manager

8/1/2019 • 12 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the **Azure Services Wizard** to simplify the process of configuring the Azure cloud services you use with Configuration Manager. This wizard provides a common configuration experience by using Azure Active Directory (Azure AD) web app registrations. These apps provide subscription and configuration details, and authenticate communications with Azure AD. The app replaces entering this same information each time you set up a new Configuration Manager component or service with Azure.

Available services

Configure the following Azure services using this wizard:

- **Cloud Management**: This service enables the site and clients to authenticate by using Azure AD. This authentication enables other scenarios, such as:
  - Install and assign Configuration Manager Windows 10 clients using Azure AD for authentication
  - Configure Azure AD User Discovery
  - Configure Azure AD User Group Discovery
  - Support certain cloud management gateway scenarios
  - App approval email notifications
- **Log Analytics Connector**: Connect to Azure Log Analytics. Sync collection data to Log Analytics.

  > **NOTE**
  > This article refers to the *Log Analytics Connector*, which was formerly called the *OMS Connector*. There's no functional difference. For more information, see Azure Management - Monitoring.

- **Upgrade Readiness Connector**: Connect to Windows Analytics Upgrade Readiness. View client upgrade compatibility data.
- **Microsoft Store for Business**: Connect to the Microsoft Store for Business. Get store apps for your organization that you can deploy with Configuration Manager.

Service details

The following table lists details about each of the services.

- **Tenants**: The number of service instances you can configure. Each instance must be a distinct Azure tenant.
- **Clouds**: All services support the global Azure cloud, but not all services support private clouds, such as the Azure US Government cloud.
- **Web app**: Whether the service uses an Azure AD app of type *Web app / API*, also referred to as a server app in Configuration Manager.
- **Native app**: Whether the service uses an Azure AD app of type *Native*, also referred to as a client app in

Configuration Manager.

- **Actions**: Whether you can import or create these apps in the Configuration Manager Azure Services Wizard.

SERVICE	TENANTS	CLOUDS	WEB APP	NATIVE APP	ACTIONS
Cloud management with Azure AD discovery	Multiple	Public, Private	✓	✓	Import, Create
Log Analytics Connector	One	Public, Private	✓	✗	Import
Upgrade Readiness	One	Public	✓	✗	Import
Microsoft Store for Business	One	Public	✓	✗	Import, Create

About Azure AD apps

Different Azure services require distinct configurations, which you make in the Azure portal. Additionally, the apps for each service can require separate permissions to Azure resources.

You can use a single app for more than one service. There's only one object to manage in Configuration Manager and Azure AD. When the security key on the app expires, you only have to refresh one key.

When you create additional Azure services in the wizard, Configuration Manager is designed to reuse information that's common between services. This behavior helps you from needing to input the same information more than once.

For more information about the required app permissions and configurations for each service, see the relevant Configuration Manager article in Available services.

For more information about Azure apps, start with the following articles:

- Authentication and authorization in Azure App Service
- Web Apps overview
- Basics of Registering an Application in Azure AD
- Register your application with your Azure Active Directory tenant

Before you begin

After you decide the service to which you want to connect, refer to the table in Service details. This table provides information you need to complete the Azure Service Wizard. Have a discussion in advance with your Azure AD administrator. Decide which of the following actions to take:

- Manually create the apps in advance in the Azure portal. Then import the app details into Configuration Manager.
- Use Configuration Manager to directly create the apps in Azure AD. To collect the necessary data from Azure AD, review the information in the other sections of this article.

Some services require the Azure AD apps to have specific permissions. Review the information for each service to

determine any required permissions. For example, before you can import a web app, an Azure administrator must first create it in the Azure portal.

When configuring Upgrade Readiness or the Log Analytics Connector, give your newly registered web app *contributor* permission on the resource group that contains the relevant workspace. This permission allows Configuration Manager to access that workspace. When assigning the permission, search for the name of the app registration in the **Add users** area of the Azure portal. This process is the same as when providing Configuration Manager with permissions to Log Analytics. An Azure administrator must assign these permissions before you import the app into Configuration Manager.

Start the Azure Services wizard

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Cloud Services**, and select the **Azure Services** node.
2. On the **Home** tab of the ribbon, in the **Azure Services** group, select **Configure Azure Services**.
3. On the **Azure Services** page of the Azure Services Wizard:
   a. Specify a **Name** for the object in Configuration Manager.
   b. Specify an optional **Description** to help you identify the service.
   c. Select the Azure service that you want to connect with Configuration Manager.
4. Select **Next** to continue to the Azure app properties page of the Azure Services Wizard.

Azure app properties

On the **App** page of the Azure Services Wizard, first select the **Azure environment** from the list. Refer to the table in Service details for which environment is currently available to the service.

The rest of the App page varies depending upon the specific service. Refer to the table in Service details for which type of app the service uses, and which action you can use.

- If the app supports both import and creates actions, select **Browse**. This action opens the Server app dialog or the Client App dialog.
- If the app only supports the import action, select **Import**. This action opens the Import Apps dialog (server) or the Import Apps dialog (client).

After you specify the apps on this page, select **Next** to continue to the Configuration or Discovery page of the Azure Services Wizard.

Web app

This app is the Azure AD type *Web app / API*, also referred to as a server app in Configuration Manager.

Server app dialog

When you select **Browse** for the **Web app** on the App page of the Azure Services Wizard, it opens the Server app dialog. It displays a list that shows the following properties of any existing web apps:

- Tenant friendly name
- App friendly name
- Service Type

There are three actions you can take from the Server app dialog:

- To reuse an existing web app, select it from the list.
- Select **Import** to open the Import apps dialog.

- Select **Create** to open the Create Server Application dialog.

After you select, import or create a web app, select **OK** to close the Server app dialog. This action returns to the App page of the Azure Services Wizard.

Import apps dialog (server)

When you select **Import** from the Server app dialog or the App page of the Azure Services Wizard, it opens the Import apps dialog. This page lets you enter information about an Azure AD web app that is already created in the Azure portal. It imports metadata about that web app into Configuration Manager. Specify the following information:

- **Azure AD Tenant Name**
- **Azure AD Tenant ID**
- **Application Name**: A friendly name for the app.
- **Client ID**
- **Secret Key**
- **Secret Key Expiry**: Select a future date from the calendar.
- **App ID URI**: This value needs to be unique in your Azure AD tenant. It is in the access token used by the Configuration Manager client to request access to the service. By default this value is `https://ConfigMgrService`.

After entering the information, select **Verify**. Then select **OK** to close the Import apps dialog. This action returns to either the App page of the Azure Services Wizard, or the Server app dialog.

Create Server Application dialog

When you select **Create** from the Server app dialog, it opens the Create Server Application dialog. This page automates the creation of a web app in Azure AD. Specify the following information:

- **Application Name**: A friendly name for the app.
- **HomePage URL**: This value isn't used by Configuration Manager, but required by Azure AD. By default this value is `https://ConfigMgrService`.
- **App ID URI**: This value needs to be unique in your Azure AD tenant. It is in the access token used by the Configuration Manager client to request access to the service. By default this value is `https://ConfigMgrService`.
- **Secret Key validity period**: choose either **1 year** or **2 years** from the drop-down list. One year is the default value.

Select **Sign in** to authenticate to Azure as an administrative user. These credentials aren't saved by Configuration Manager. This persona doesn't require permissions in Configuration Manager, and doesn't need to be the same account that runs the Azure Services Wizard. After successfully authenticating to Azure, the page shows the **Azure AD Tenant Name** for reference.

Select **OK** to create the web app in Azure AD and close the Create Server Application dialog. This action returns to the Server app dialog.

Native Client app

This app is the Azure AD type *Native*, also referred to as a client app in Configuration Manager.

Client App dialog

When you select **Browse** for the **Native Client app** on the App page of the Azure Services Wizard, it opens the Client App dialog. It displays a list that shows the following properties of any existing native apps:

- Tenant friendly name
- App friendly name
- Service Type

There are three actions you can take from the Client App dialog:

- To reuse an existing native app, select it from the list.
- Select **Import** to open the Import apps dialog.
- Select **Create** to open the Create Client Application dialog.

After you select, import or create a native app, choose **OK** to close the Client App dialog. This action returns to the App page of the Azure Services Wizard.

Import apps dialog (client)

When you select **Import** from the Client App dialog, it opens the Import apps dialog. This page lets you enter information about an Azure AD native app that is already created in the Azure portal. It imports metadata about that native app into Configuration Manager. Specify the following information:

- **Application Name**: A friendly name for the app.
- **Client ID**

After entering the information, select **Verify**. Then select **OK** to close the Import apps dialog. This action returns to the Client App dialog.

Create Client Application dialog

When you select **Create** from the Client App dialog, it opens the Create Client Application dialog. This page automates the creation of a native app in Azure AD. Specify the following information:

- **Application Name**: A friendly name for the app.
- **Reply URL**: This value isn't used by Configuration Manager, but required by Azure AD. By default this value is `https://ConfigMgrService`.

Select **Sign in** to authenticate to Azure as an administrative user. These credentials aren't saved by Configuration Manager. This persona doesn't require permissions in Configuration Manager, and doesn't need to be the same account that runs the Azure Services Wizard. After successfully authenticating to Azure, the page shows the **Azure AD Tenant Name** for reference.

Select **OK** to create the native app in Azure AD and close the Create Client Application dialog. This action returns to the Client App dialog.

Configuration or Discovery

After specifying the web and native apps on the Apps page, the Azure Services Wizard proceeds to either a **Configuration** or **Discovery** page, depending upon the service to which you're connecting. The details of this page vary from service to service. For more information, see one of the following articles:

- **Cloud Management** service, **Discovery** page: Configure Azure AD User Discovery
- **Log Analytics Connector** service, **Configuration** page: Configure the connection to Log Analytics
- **Upgrade Readiness Connector** service, **Configuration** page: Use the Azure Wizard to create the connection
- **Microsoft Store for Business** service, **Configurations** page: Configure Microsoft Store for Business synchronization

Finally, complete the Azure Services Wizard through the Summary, Progress, and Completion pages. You've completed the configuration of an Azure service in Configuration Manager. Repeat this process to configure other Azure services.

Renew secret key

> **NOTE**
> To renew the secret key of an Azure app in version 1802 and earlier, you need to recreate the app.

Renew key for created app

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Cloud Services**, and select the **Azure Active Directory Tenants** node.
2. On the Details pane, select the Azure AD tenant for the app.
3. In the ribbon, select **Renew Secret Key**. Enter the credentials of either the app owner or an Azure AD administrator.

Renew key for imported app

If you imported the Azure app in Configuration Manager, use the Azure portal to renew. Note the new secret key and expiry date. Add this information on the **Renew Secret Key** wizard.

> **NOTE**
> Save the secret key before closing the Azure application properties **Key** page. This information is removed when you close the page.

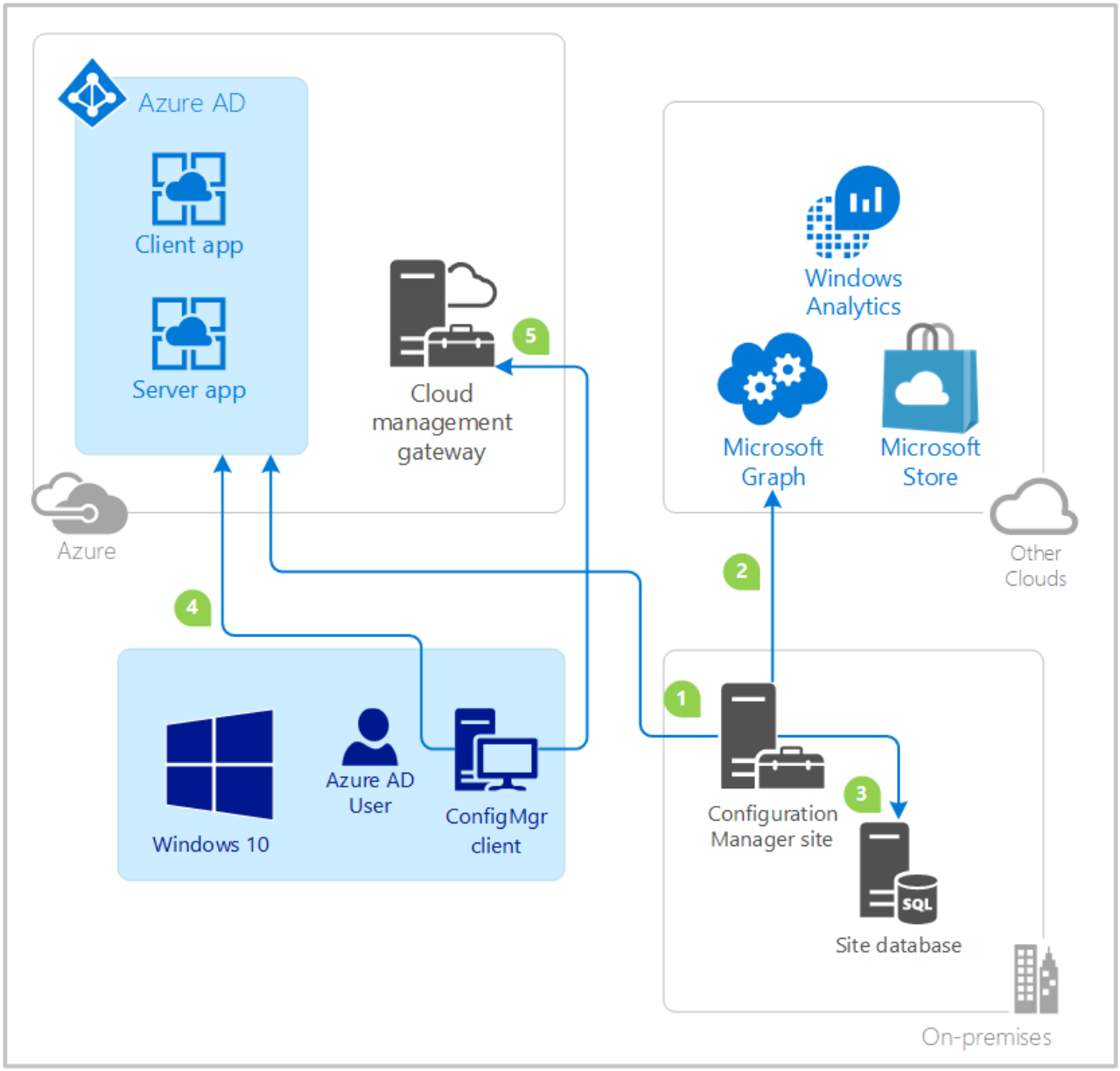
View the configuration of an Azure service

View the properties of an Azure service you've configured for use. In the Configuration Manager console, go to the **Administration** workspace, expand **Cloud Services**, and select **Azure Services**. Select the service you want to view or edit, and then select **Properties**.

If you select a service and then choose **Delete** in the ribbon, this action deletes the connection in Configuration Manager. It doesn't remove the app in Azure AD. Ask your Azure administrator to delete the app when it's no longer needed. Or run the Azure Service Wizard to import the app.

Cloud management data flow

The following diagram is a conceptual data flow for the interaction between Configuration Manager, Azure AD, and connected cloud services. This specific example uses the **Cloud Management** service, which includes a Windows 10 client, and both server and client apps. The flows for other services are similar.



1. The Configuration Manager administrator imports or creates the client and server apps in Azure AD.
2. Configuration Manager Azure AD user discovery method runs. The site uses the Azure AD server app token to query Microsoft Graph for user objects.
3. The site stores data about the user objects. For more information, see Azure AD User Discovery.
4. The Configuration Manager client requests the Azure AD user token. The client makes the claim using the application ID of the Azure AD client app, and the server app as the audience. For more information, see Claims in Azure AD Security Tokens.
5. The client authenticates with the site by presenting the Azure AD token to the cloud management gateway and on-premises HTTPS-enabled management point.

Accounts used in Configuration Manager

7/19/2019 • 25 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the following information to identify the Windows groups, accounts, and SQL objects that are used in Configuration Manager, how they are used, and any requirements.

- Windows groups that Configuration Manager creates and uses
  - ConfigMgr_CollectedFilesAccess
  - ConfigMgr_DViewAccess
  - ConfigMgr Remote Control Users
  - SMS Admins
  - SMS_SiteSystemToSiteServerConnection_MP_<sitecode>
  - SMS_SiteSystemToSiteServerConnection_SMSProv_<sitecode>
  - SMS_SiteSystemToSiteServerConnection_Stat_<sitecode>
  - SMS_SiteToSiteConnection_<sitecode>
- Accounts that Configuration Manager uses
  - Active Directory group discovery account
  - Active Directory system discovery account
  - Active Directory user discovery account
  - Active Directory forest account
  - Certificate registration point account
  - Capture OS image account
  - Client push installation account
  - Enrollment point connection account
  - Exchange Server connection account
  - Management point connection account
  - Multicast connection account
  - Network access account
  - Package access account
  - Reporting services point account
  - Remote tools permitted viewer accounts
  - Site installation account
  - Site system installation account
  - Site system proxy server account
  - SMTP server connection account
  - Software update point connection account
  - Source site account
  - Source site database account
  - Task sequence domain join account
  - Task sequence network folder connection account
  - Task sequence run as account
- User Objects that Configuration Manager uses in SQL

- smsdbuser_ReadOnly
- smsdbuser_ReadWrite
- smsdbuser_ReportSchema

Windows groups that Configuration Manager creates and uses

Configuration Manager automatically creates, and in many cases automatically maintains, the following Windows groups:

> **NOTE**
> When Configuration Manager creates a group on a computer that's a domain member, the group is a local security group. If the computer is a domain controller, the group is a domain local group. This type of group is shared among all domain controllers in the domain.

ConfigMgr_CollectedFilesAccess

Configuration Manager uses this group to grant access to view files collected by software inventory.

For more information, see Introduction to software inventory.

Type and location

This group is a local security group created on the primary site server.

When you uninstall a site, this group isn't automatically removed. Manually delete it after uninstalling a site.

Membership

Configuration Manager automatically manages the group membership. Membership includes administrative users that are granted the **View Collected Files** permission to the **Collection** securable object from an assigned security role.

Permissions

By default, this group has **Read** permission to the following folder on the site server:

```
C:\Program Files\Microsoft Configuration Manager\sinv.box\FileCol
```

ConfigMgr_DViewAccess

This group is a local security group that Configuration Manager creates on the site database server or database replica server for a child primary site. The site creates it when you use distributed views for database replication between sites in a hierarchy. It contains the site server and SQL Server computer accounts of the central administration site.

For more information, see Data transfers between sites.

ConfigMgr Remote Control Users

Configuration Manager remote tools use this group to store the accounts and groups that you set up in the **Permitted Viewers** list. The site assigns this list to each client.

For more information, see Introduction to remote control.

Type and location

This group is a local security group created on the Configuration Manager client when the client receives a policy that enables remote tools.

After you disable remote tools for a client, this group isn't automatically removed. Manually delete it after disabling remote tools.

Membership

By default, there are no members in this group. When you add users to the **Permitted Viewers** list, they're

automatically added to this group.

Use the **Permitted Viewers** list to manage the membership of this group instead of adding users or groups directly to this group.

In addition to being a permitted viewer, an administrative user must have the **Remote Control** permission to the **Collection** object. Assign this permission by using the **Remote Tools Operator** security role.

Permissions

By default, this group doesn't have permissions to any locations on the computer. It's used only to hold the **Permitted Viewers** list.

SMS Admins

Configuration Manager uses this group to grant access to the SMS Provider through WMI. Access to the SMS Provider is required to view and change objects in the Configuration Manager console.

> **NOTE**
> The role-based administration configuration of an administrative user determines which objects they can view and manage when using the Configuration Manager console.

For more information, see Plan for the SMS Provider.

Type and location

This group is a local security group created on each computer that has an SMS Provider.

When you uninstall a site, this group isn't automatically removed. Manually delete it after uninstalling a site.

Membership

Configuration Manager automatically manages the group membership. By default, each administrative user in a hierarchy and the site server computer account are members of the **SMS Admins** group on each SMS Provider computer in a site.

Permissions

You can view the rights and permissions for the SMS Admins group in the **WMI Control** MMC snap-in. By default, this group is granted **Enable Account** and **Remote Enable** on the `Root\SMS` WMI namespace. Authenticated users have **Execute Methods**, **Provider Write**, and **Enable Account**.

When you use a remote Configuration Manager console, configure **Remote Activation** DCOM permissions on both the site server computer and the SMS Provider. Grant these rights to the **SMS Admins** group. This action simplifies administration instead of granting these rights directly to users or groups. For more information, see Configure DCOM permissions for remote Configuration Manager consoles.

SMS_SiteSystemToSiteServerConnection_MP_<sitecode>

Management points that are remote from the site server use this group to connect to the site database. This group provides a management point access to the inbox folders on the site server and the site database.

Type and location

This group is a local security group created on each computer that has an SMS Provider.

When you uninstall a site, this group isn't automatically removed. Manually delete it after uninstalling a site.

Membership

Configuration Manager automatically manages the group membership. By default, membership includes the computer accounts of remote computers that have a management point for the site.

Permissions

By default, this group has **Read**, **Read & execute**, and **List folder contents** permission to the following folder on

the site server: `C:\Program Files\Microsoft Configuration Manager\inboxes`. This group has the additional permission of **Write** to subfolders below **inboxes**, to which the management point writes client data.

SMS_SiteSystemToSiteServerConnection_SMSProv_<sitecode>

Remote SMS Provider computers use this group to connect to the site server.

Type and location

This group is a local security group created on the site server.

When you uninstall a site, this group isn't automatically removed. Manually delete it after uninstalling a site.

Membership

Configuration Manager automatically manages the group membership. By default, membership includes the computer account or a domain user account. It uses this account to connect to the site server from each remote SMS Provider.

Permissions

By default, this group has **Read**, **Read & execute**, and **List folder contents** permission to the following folder on the site server: `C:\Program Files\Microsoft Configuration Manager\inboxes`. This group has the additional permissions of **Write** and **Modify** to subfolders below the inboxes. The SMS Provider requires access to these folders.

This group also has **Read** permission to the subfolders on the site server below `C:\Program Files\Microsoft Configuration Manager\OSD\Bin`.

It also has the following permissions to the subfolders below `C:\Program Files\Microsoft Configuration Manager\OSD\boot`:

- **Read**
- **Read & execute**
- **List folder contents**
- **Write**
- **Modify**

SMS_SiteSystemToSiteServerConnection_Stat_<sitecode>

The file dispatch manager component on Configuration Manager remote site system computers uses this group to connect to the site server.

Type and location

This group is a local security group created on the site server.

When you uninstall a site, this group isn't automatically removed. Manually delete it after uninstalling a site.

Membership

Configuration Manager automatically manages the group membership. By default, membership includes the computer account or the domain user account. It uses this account to connect to the site server from each remote site system that runs the file dispatch manager.

Permissions

By default, this group has **Read**, **Read & execute**, and **List folder contents** permission to the following folder and its subfolders on the site server: `C:\Program Files\Microsoft Configuration Manager\inboxes`.

This group has the additional permissions of **Write** and **Modify** to the following folder on the site server: `C:\Program Files\Microsoft Configuration Manager\inboxes\statmgr.box`.

SMS_SiteToSiteConnection_<sitecode>

Configuration Manager uses this group to enable file-based replication between sites in a hierarchy. For each remote site that directly transfers files to this site, this group has accounts set up as a **File Replication Account**.

Type and location

This group is a local security group created on the site server.

Membership

When you install a new site as a child of another site, Configuration Manager automatically adds the computer account of the new site server to this group on the parent site server. Configuration Manager also adds the parent site's computer account to the group on the new site server. If you specify another account for file-based transfers, add that account to this group on the destination site server.

When you uninstall a site, this group isn't automatically removed. Manually delete it after uninstalling a site.

Permissions

By default, this group has **Full control** to the following folder:

`C:\Program Files\Microsoft Configuration Manager\inboxes\despoolr.box\receive`.

Accounts that Configuration Manager uses

You can set up the following accounts for Configuration Manager.

Active Directory group discovery account

The site uses the **Active Directory group discovery account** to discover the following objects from the locations in Active Directory Domain Services that you specify:

- Local, global, and universal security groups
- The membership within these groups
- The membership within distribution groups
  - Distribution groups aren't discovered as group resources

This account can be a computer account of the site server that runs discovery, or a Windows user account. It must have **Read** access permission to the Active Directory locations that you specify for discovery.

For more information, see Active Directory group discovery.

Active Directory system discovery account

The site uses the **Active Directory system discovery account** to discover computers from the locations in Active Directory Domain Services that you specify.

This account can be a computer account of the site server that runs discovery, or a Windows user account. It must have **Read** access permission to the Active Directory locations that you specify for discovery.

For more information, see Active Directory system discovery.

Active Directory user discovery account

The site uses the **Active Directory user discovery account** to discover user accounts from the locations in Active Directory Domain Services that you specify.

This account can be a computer account of the site server that runs discovery, or a Windows user account. It must have **Read** access permission to the Active Directory locations that you specify for discovery.

For more information, see Active Directory user discovery.

Active Directory forest account

The site uses the **Active Directory forest account** to discover network infrastructure from Active Directory forests. Central administration sites and primary sites also use it to publish site data to Active Directory Domain Services for a forest.

> **NOTE**
> Secondary sites always use the secondary site server computer account to publish to Active Directory.

To discover and publish to untrusted forests, the Active Directory forest account must be a global account. If you don't use the computer account of the site server, you can select only a global account.

This account must have **Read** permissions to each Active Directory forest where you want to discover network infrastructure.

This account must have **Full Control** permissions to the **System Management** container and all its child objects in each Active Directory forest where you want to publish site data. For more information, see Prepare Active Directory for site publishing.

For more information, see Active Directory forest discovery.

Certificate registration point account

The certificate registration point uses the **Certificate registration point account** to connect to the Configuration Manager database. It uses its computer account by default, but you can configure a user account instead. When the certificate registration point is in an untrusted domain from the site server, you must specify a user account. This account requires only **Read** access to the site database, because the state message system handles write tasks.

For more information, see Introduction to certificate profiles.

Capture OS image account

When you capture an OS image, Configuration Manager uses the **Capture OS image account** to access the folder where you store captured images. If you add the **Capture OS Image** step to a task sequence, this account is required.

The account must have **Read** and **Write** permissions on the network share where you store captured images.

If you change the password for the account in Windows, update the task sequence with the new password. The Configuration Manager client receives the new password when it next downloads the client policy.

If you need to use this account, create one domain user account. Grant it minimal permissions to access the required network resources, and use it for all capture task sequences.

> **IMPORTANT**
> Don't assign interactive sign-in permissions to this account.
>
> Don't use the network access account for this account.

For more information, see Create a task sequence to capture an OS.

Client push installation account

When you deploy clients by using the client push installation method, the site uses the **Client push installation account** to connect to computers and install the Configuration Manager client software. If you don't specify this account, the site server tries to use its computer account.

This account must be a member of the local **Administrators** group on the target client computers. This account doesn't require **Domain Admin** rights.

You can specify more than one client push installation account. Configuration Manager tries each one in turn until one succeeds.

TIP

If you have a large Active Directory environment and need to change this account, use the following process to more effectively coordinate this account update:

1. Create a new account with a different name
2. Add the new account to the list of client push installation accounts in Configuration Manager
3. Allow sufficient time for Active Directory Domain Services to replicate the new account
4. Then remove the old account from Configuration Manager and Active Directory Domain Services

IMPORTANT

Don't grant this account the right to sign in locally.

For more information, see Client push installation.

Enrollment point connection account

The enrollment point uses the **Enrollment point connection account** to connect to the Configuration Manager site database. It uses its computer account by default, but you can configure a user account instead. When the enrollment point is in an untrusted domain from the site server, you must specify a user account. This account requires **Read** and **Write** access to the site database.

For more information, see Install site system roles for on-premises MDM.

Exchange Server connection account

The site server uses the **Exchange Server connection account** to connect to the specified Exchange Server. It uses this connection to find and manage mobile devices that connect to Exchange Server. This account requires Exchange PowerShell cmdlets that provide the required permissions to the Exchange Server computer. For more information about the cmdlets, see Manage mobile devices with Configuration Manager and Exchange.

Management point connection account

The management point uses the **Management point connection account** to connect to the Configuration Manager site database. It uses this connection to send and retrieve information for clients. The management point uses its computer account by default, but you can configure a user account instead. When the management point is in an untrusted domain from the site server, you must specify a user account.

Create the account as a low-rights, local account on the computer that runs Microsoft SQL Server.

IMPORTANT

Don't grant interactive sign-in rights to this account.

Multicast connection account

Multicast-enabled distribution points use the **Multicast connection account** to read information from the site database. The server uses its computer account by default, but you can configure a user account instead. When the site database is in an untrusted forest, you must specify a user account. For example, if your data center has a perimeter network in a forest other than the site server and site database, use this account to read the multicast information from the site database.

If you need this account, create it as a low-rights, local account on the computer that runs Microsoft SQL Server.

> **IMPORTANT**
>
> Don't grant interactive sign-in rights to this account.

For more information, see Use multicast to deploy Windows over the network.

Network access account

Client computers use the **network access account** when they can't use their local computer account to access content on distribution points. It mostly applies to workgroup clients and computers from untrusted domains. This account is also used during OS deployment, when the computer that's installing the OS doesn't yet have a computer account on the domain.

> **IMPORTANT**
>
> The network access account is never used as the security context to run programs, install software updates, or run task sequences. It's used only for accessing resources on the network.

A Configuration Manager client first tries to use its computer account to download the content. If it fails, it then automatically tries the network access account.

Starting in version 1806, a workgroup or Azure AD-joined client can securely access content from distribution points without the need for a network access account. This behavior includes OS deployment scenarios with a task sequence running from boot media, PXE, or Software Center. For more information, see Enhanced HTTP.

> **NOTE**
>
> If you enable **Enhanced HTTP** to not require the network access account, the distribution point needs to be running Windows Server 2008 R2 SP1 or later.
>
> Upgrade clients to at least version 1806 before enabling this functionality. If you only allow **Enhanced HTTP** connections, older clients can't authenticate using this method, so can't download the client upgrade package from a distribution point.

Permissions

Grant this account the minimum appropriate permissions on the content that the client requires to access the software. The account must have the **Access this computer from the network** right on the distribution point. You can configure up to 10 network access accounts per site.

Create the account in any domain that provides the necessary access to resources. The network access account must always include a domain name. Pass-through security isn't supported for this account. If you have distribution points in multiple domains, create the account in a trusted domain.

> **TIP**
>
> To avoid account lockouts, don't change the password on an existing network access account. Instead, create a new account and set up the new account in Configuration Manager. When sufficient time has passed for all clients to have received the new account details, remove the old account from the network shared folders and delete the account.

> **IMPORTANT**
>
> Don't grant interactive sign-in rights to this account.
>
> Don't grant this account the right to join computers to the domain. If you must join computers to the domain during a task sequence, use the Task sequence domain join account.

Configure the network access account

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. Then select the site.
2. On the **Settings** group of the ribbon, select **Configure Site Components**, and choose **Software Distribution**.
3. Choose the **Network access account** tab. Set up one or more accounts, and then choose **OK**.

Package access account

A **Package access account** lets you set NTFS permissions to specify the users and user groups that can access package content on distribution points. By default, Configuration Manager grants access only to the generic access accounts **User** and **Administrator**. You can control access for client computers by using additional Windows accounts or groups. Mobile devices always retrieve package content anonymously, so they don't use a package access account.

By default, when Configuration Manager copies the content files to a distribution point, it grants **Read** access to the local **Users** group, and **Full Control** to the local **Administrators** group. The actual permissions required depend on the package. If you have clients in workgroups or in untrusted forests, those clients use the network access account to access the package content. Make sure that the network access account has permissions to the package by using the defined package access accounts.

Use accounts in a domain that can access the distribution points. If you create or modify the account after you create the package, you must redistribute the package. Updating the package doesn't change the NTFS permissions on the package.

You don't have to add the network access account as a package access account, because membership of the **Users** group adds it automatically. Restricting the package access account to only the network access account doesn't prevent clients from accessing the package.

Manage package access accounts

1. In the Configuration Manager console, choose **Software Library**.
2. In the **Software Library** workspace, determine the type of content for which you want to manage access accounts, and follow the steps provided:
   - **Application**: Expand **Application Management**, choose **Applications**, and then select the application for which to manage access accounts.
   - **Package**: Expand **Application Management**, choose **Packages**, and then select the package for which to manage access accounts.
   - **Software update deployment package**: Expand **Software Updates**, choose **Deployment Packages**, and then select the deployment package for which to manage access accounts.
   - **Driver package**: Expand **Operating Systems**, choose **Driver Packages**, and then select the driver package for which to manage access accounts.
   - **OS image**: Expand **Operating Systems**, choose **Operating System Images**, and then select the operating system image for which to manage access accounts.
   - **OS upgrade package**: Expand **Operating Systems**, choose **Operating system upgrade packages**, and then select the OS upgrade package for which to manage access accounts.
   - **Boot image**: Expand **Operating Systems**, choose **Boot Images**, and then select the boot image for which to manage access accounts.
3. Right-click the selected object, and then choose **Manage Access Accounts**.

4. In the **Add Account** dialog box, specify the account type that will be granted access to the content, and then specify the access rights associated with the account.

> **NOTE**
> When you add a user name for the account, and Configuration Manager finds both a local user account and a domain user account with that name, Configuration Manager sets access rights for the domain user account.

Reporting services point account

SQL Server Reporting Services uses the **Reporting services point account** to retrieve the data for Configuration Manager reports from the site database. The Windows user account and password that you specify are encrypted and stored in the SQL Server Reporting Services database.

> **NOTE**
> The account you specify must have **Log on locally** permissions on the computer hosting the SQL Reporting Services database.

For more information, see Introduction to reporting.

Remote tools permitted viewer accounts

The accounts that you specify as **Permitted Viewers** for remote control are a list of users who are allowed to use remote tools functionality on clients.

For more information, see Introduction to remote control.

Site installation account

Use a domain user account to sign in to the server where you run Configuration Manager setup and install a new site.

This account requires the following rights:

- **Administrator** on the following servers:
  - The site server
  - Each server that hosts the site database
  - Each instance of the SMS Provider for the site
- **Sysadmin** on the instance of SQL Server that hosts the site database

Configuration Manager setup automatically adds this account to the SMS Admins group.

After installation, this account is the only user with rights to the Configuration Manager console. If you need to remove this account, make sure to add its rights to another user first.

When expanding a standalone site to include a central administration site, this account requires either **Full Administrator** or **Infrastructure Administrator** role-based administration rights at the standalone primary site.

Site system installation account

The site server uses the **Site system installation account** to install, reinstall, uninstall, and set up site systems. If you set up the site system to require the site server to initiate connections to this site system, Configuration Manager also uses this account to pull data from the site system after it installs the site system and any roles. Each site system can have a different installation account, but you can set up only one installation account to manage all roles on that site system.

This account requires local administrative permissions on the target site systems. Additionally, this account must

have **Access this computer from the network** in the security policy on the target site systems.

> **TIP**
>
> If you have many domain controllers and these accounts are used across domains, before you set up the site system, check that Active Directory has replicated these accounts.
>
> When you specify a local account on each site system to be managed, this configuration is more secure than using domain accounts. It limits the damage that attackers can do if the account is compromised. However, domain accounts are easier to manage. Consider the trade-off between security and effective administration.

Site system proxy server account

The following site system roles use the **Site system proxy server account** to access the internet via a proxy server or firewall that requires authenticated access:

- Asset Intelligence synchronization point
- Exchange Server connector
- Service connection point
- Software update point

> **IMPORTANT**
>
> Specify an account that has the least possible permissions for the required proxy server or firewall.

For more information, see Proxy server support.

SMTP server connection account

The site server uses the **SMTP server connection account** to send email alerts when the SMTP server requires authenticated access.

> **IMPORTANT**
>
> Specify an account that has the least possible permissions to send emails.

For more information, see Use alerts and the status system.

Software update point connection account

The site server uses the **Software update point connection account** for the following two software update services:

- Windows Server Update Services (WSUS), which sets up settings like product definitions, classifications, and upstream settings.
- WSUS Synchronization Manager, which requests synchronization to an upstream WSUS server or Microsoft Update.

The site system installation account can install components for software updates, but it can't perform software update-specific functions on the software update point. If you can't use the site server computer account for this functionality because the software update point is in an untrusted forest, you must specify this account in addition to the site system installation account.

This account must be a local administrator on the computer where you install WSUS. It must also be part of the local **WSUS Administrators** group.

For more information, see Plan for software updates.

Source site account

The migration process uses the **Source site account** to access the SMS Provider of the source site. This account requires **Read** permissions to site objects in the source site to gather data for migration jobs.

If you have Configuration Manager 2007 distribution points or secondary sites with colocated distribution points, when you upgrade them to Configuration Manager (current branch) distribution points, this account must also have **Delete** permissions to the **Site** class. This permission is to successfully remove the distribution point from the Configuration Manager 2007 site during the upgrade.

> **NOTE**
> Both the source site account and the source site database account are identified as **Migration Manager** in the **Accounts** node of the **Administration** workspace in the Configuration Manager console.

For more information, see Migrate data between hierarchies.

Source site database account

The migration process uses the **Source site database account** to access the SQL Server database for the source site. To gather data from the SQL Server database of the source site, the source site database account must have the **Read** and **Execute** permissions to the source site's SQL Server database.

If you use the Configuration Manager (current branch) computer account, make sure that all the following are true for this account:

- It's a member of the **Distributed COM Users** security group in the same domain as the Configuration Manager 2007 site
- It's a member of the **SMS Admins** security group
- It has the **Read** permission to all Configuration Manager 2007 objects

> **NOTE**
> Both the source site account and the source site database account are identified as **Migration Manager** in the **Accounts** node of the **Administration** workspace in the Configuration Manager console.

For more information, see Migrate data between hierarchies.

Task sequence domain join account

Windows Setup uses the **Task sequence domain join account** to join a newly imaged computer to a domain. This account is required by the Join Domain or Workgroup task sequence step with the **Join a domain** option. This account can also be set up with the Apply Network Settings step, but it isn't required.

This account requires the **Domain Join** right in the target domain.

> **TIP**
> Create one domain user account with the minimal permissions to join the domain, and use it for all task sequences.

> **IMPORTANT**
> Don't assign interactive sign-in permissions to this account.
>
> Don't use the network access account for this account.

Task sequence network folder connection account

The task sequence engine uses the **Task sequence network folder connection account** to connect to a shared folder on the network. This account is required by the Connect to Network Folder task sequence step.

This account requires permissions to access the specified shared folder. It must be a domain user account.

> **TIP**
> Create one domain user account with minimal permissions to access the required network resources, and use it for all task sequences.

> **IMPORTANT**
> Don't assign interactive sign-in permissions to this account.
>
> Don't use the network access account for this account.

Task sequence run as account

The task sequence engine uses the **Task sequence run as account** to run command lines or PowerShell Scripts with credentials other than the Local System account. This account is required by the Run Command Line and Run PowerShell Script task sequence steps with the option **Run this step as the following account** chosen.

Set up the account to have the minimum permissions required to run the command line that you specify in the task sequence. The account requires interactive sign-in rights. It usually requires the ability to install software and access network resources. For the Run PowerShell Script task, this account requires local administrator permissions.

> **IMPORTANT**
> Don't use the network access account for this account.
>
> Never make the account a domain admin.
>
> Never set up roaming profiles for this account. When the task sequence runs, it downloads the roaming profile for the account. This leaves the profile vulnerable to access on the local computer.
>
> Limit the scope of the account. For example, create different task sequence run as accounts for each task sequence. Then if one account is compromised, only the client computers to which that account has access are compromised.
>
> If the command line requires administrative access on the computer, consider creating a local administrator account solely for this account on all computers that run the task sequence. Delete the account once you no longer need it.

User Objects that Configuration Manager uses in SQL

Configuration Manager automatically creates and maintains the following user objects in SQL. These objects are located within the Configuration Manager database under Security/Users.

> **IMPORTANT**
> Modifying or removing these objects may cause drastic issues within a Configuration Manager environment. We recommend you do not make any changes to these objects.

smsdbuser_ReadOnly

This object is used to run queries under the read-only context. This object is leveraged with several stored procedures.

smsdbuser_ReadWrite

This object is used to provide permissions for dynamic SQL statements.

smsdbuser_ReportSchema

This object is used to run SQL Reporting Executions. The following stored procedure is used with this function: spSRExecQuery.

Communications between endpoints in Configuration Manager

2/12/2019 • 14 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article describes how Configuration Manager site systems and clients communicate across your network. It includes the following sections:

Communications between site systems in a site

When Configuration Manager site systems or components communicate across the network to other site systems or components in the site, they use one of the following protocols, depending on how you configure the site:

- Server message block (SMB)
- HTTP
- HTTPS

With the exception of communication from the site server to a distribution point, server-to-server communications in a site can occur at any time. These communications don't use mechanisms to control the network bandwidth. Because you can't control the communication between site systems, make sure that you install site system servers in locations that have fast and well-connected networks.

Site server to distribution point

To help you manage the transfer of content from the site server to distribution points, use the following strategies:

- Configure the distribution point for network bandwidth control and scheduling. These controls resemble the configurations that are used by intersite addresses. Use this configuration instead of installing another Configuration Manager site when the transfer of content to remote network locations is your main bandwidth consideration.
- You can install a distribution point as a prestaged distribution point. A prestaged distribution point lets you use content that is manually put on the distribution point server and removes the requirement to transfer content files across the network.

For more information, see Manage network bandwidth for content management.

Communications from clients to site systems and services

Clients initiate communication to site system roles, Active Directory Domain Services, and online services. To enable these communications, firewalls must allow the network traffic between clients and the endpoint of their communications. For more information about ports and protocols used by clients when they communicate to these endpoints, see Ports used in Configuration Manager.

Before a client can communicate with a site system role, the client uses service location to find a role that supports the client's protocol (HTTP or HTTPS). By default, clients use the most secure method that's available to them. For more information, see Understand how clients find site resources and services.

To use HTTPS, configure one of the following options:

- Use a public key infrastructure (PKI) and install PKI certificates on clients and servers. For information about how to use certificates, see PKI certificate requirements.
- Starting in version 1806, configure the site to **Use Configuration Manager-generated certificates for HTTP site systems**. For more information, see Enhanced HTTP.

When you deploy a site system role that uses Internet Information Services (IIS) and supports communication from clients, you must specify whether clients connect to the site system by using HTTP or HTTPS. If you use HTTP, you must also consider signing and encryption choices. For more information, see Planning for signing and encryption.

Client to management point communication

There are two stages when a client communicates with a management point: authentication (transport) and authorization (message). This process varies depending upon the following factors:

- Site configuration: HTTP, HTTPS, or enhanced HTTP
- Management point configuration: HTTPS only, or allows HTTP or HTTPS
- Device identity for device-centric scenarios
- User identity for user-centric scenarios

Use the following table to understand how this process works:

MP TYPE	CLIENT AUTHENTICATION	CLIENT AUTHORIZATION DEVICE IDENTITY	CLIENT AUTHORIZATION USER IDENTITY
HTTP	Anonymous With Enhanced HTTP, the site verifies the Azure AD *user* or *device* token.	Location request: Anonymous Client package: Anonymous Registration, using one of the following methods to prove device identity: - Anonymous (manual approval) - Windows-integrated authentication - Azure AD *device* token (Enhanced HTTP) After registration, the client uses message signing to prove device identity	For user-centric scenarios, using one of the following methods to prove user identity: - Windows-integrated authentication - Azure AD *user* token (Enhanced HTTP)

MP TYPE	CLIENT AUTHENTICATION	CLIENT AUTHORIZATION DEVICE IDENTITY	CLIENT AUTHORIZATION USER IDENTITY
HTTPS	Using one of the following methods: - PKI certificate - Windows-integrated authentication - Azure AD *user* or *device* token	Location request: Anonymous Client package: Anonymous Registration, using one of the following methods to prove device identity: - Anonymous (manual approval) - Windows-integrated authentication - PKI certificate - Azure AD *user* or *device* token After registration, the client uses message signing to prove device identity	For user-centric scenarios, using one of the following methods to prove user identity: - Windows-integrated authentication - Azure AD *user* token

> **TIP**
> For more information on the configuration of the management point for different device identity types and with the cloud management gateway, see Enable management point for HTTPS.

Client to distribution point communication

When a client communicates with a distribution point, it only needs to authenticate before downloading the content. Use the following table to understand how this process works:

DP TYPE	CLIENT AUTHENTICATION
HTTP	- Anonymous, if allowed - Windows-integrated authentication with computer account or network access account - Content access token (Enhanced HTTP)
HTTPS	- PKI certificate - Windows-integrated authentication with computer account or network access account - Content access token

Considerations for client communications from the internet or an untrusted forest

The following site system roles installed at primary sites support connections from clients that are in untrusted locations, such as the internet or an untrusted forest. (Secondary sites don't support client connections from untrusted locations.)

- Application catalog website point
- Configuration Manager policy module (NDES)
- Distribution point
- Cloud-based distribution point (requires HTTPS)
- Enrollment proxy point
- Fallback status point
- Management point

- Software update point
- Cloud management gateway (requires HTTPS)

About internet-facing site systems

> **NOTE**
> The following section is about internet-based client management scenarios. It doesn't apply to cloud management gateway scenarios. For more information, see Manage clients on the internet.

There's no requirement to have a trust between a client's forest and that of the site system server. However, when the forest that contains an internet-facing site system trusts the forest that contains the user accounts, this configuration supports user-based policies for devices on the internet when you enable the **Client Policy** client setting **Enable user policy requests from internet clients**.

For example, the following configurations illustrate when internet-based client management supports user policies for devices on the internet:

- The internet-based management point is in the perimeter network where a read-only domain controller resides to authenticate the user and an intervening firewall allows Active Directory packets.
- The user account is in Forest A (the intranet) and the internet-based management point is in Forest B (the perimeter network). Forest B trusts Forest A, and an intervening firewall allows the authentication packets.
- The user account and the internet-based management point are in Forest A (the intranet). The management point is published to the internet by using a web proxy server (like Forefront Threat Management Gateway).

> **NOTE**
> If Kerberos authentication fails, NTLM authentication is then automatically tried.

As the previous example shows, you can place internet-based site systems in the intranet when they're published to the internet by using a web proxy server. These site systems can be configured for client connection from the internet only, or for client connections from the internet and intranet. When you use a web proxy server, you can configure it for Secure Sockets Layer (SSL) bridging to SSL (more secure) or SSL tunneling as follows:

- **SSL bridging to SSL:**
  The recommended configuration when you use proxy web servers for internet-based client management is SSL bridging to SSL, which uses SSL termination with authentication. Client computers must be authenticated by using computer authentication, and mobile device legacy clients are authenticated by using user authentication. Mobile devices that are enrolled by Configuration Manager don't support SSL bridging.

  The benefit of SSL termination at the proxy web server is that packets from the internet are subject to inspection before they're forwarded to the internal network. The proxy web server authenticates the connection from the client, terminates it, and then opens a new authenticated connection to the internet-based site systems. When Configuration Manager clients use a proxy web server, the client identity (client GUID) is securely contained in the packet payload so that the management point doesn't consider the proxy web server to be the client. Bridging isn't supported in Configuration Manager with HTTP to HTTPS, or from HTTPS to HTTP.

- **Tunneling**:
  If your proxy web server can't support the requirements for SSL bridging, or you want to configure internet support for mobile devices that are enrolled by Configuration Manager, SSL tunneling is also supported. It's a less secure option because the SSL packets from the internet are forwarded to the site systems without SSL termination, so they can't be inspected for malicious content. When you use SSL tunneling, there are no

certificate requirements for the proxy web server.

Communications across Active Directory forests

Configuration Manager supports sites and hierarchies that span Active Directory forests. It also supports domain computers that aren't in the same Active Directory forest as the site server, and computers that are in workgroups.

Support domain computers in a forest that's not trusted by your site server's forest

- Install site system roles in that untrusted forest, with the option to publish site information to that Active Directory forest
- Manage these computers as if they're workgroup computers

When you install site system servers in an untrusted Active Directory forest, the client-to-server communication from clients in that forest is kept within that forest, and Configuration Manager can authenticate the computer by using Kerberos. When you publish site information to the client's forest, clients benefit from retrieving site information, such as a list of available management points, from their Active Directory forest, rather than downloading this information from their assigned management point.

> **NOTE**
> If you want to manage devices that are on the internet, you can install internet-based site system roles in your perimeter network when the site system servers are in an Active Directory forest. This scenario doesn't require two-way trust between the perimeter network and the site server's forest.

Support computers in a workgroup

- Manually approve workgroup computers when they use HTTP client connections to site system roles. Configuration Manager can't authenticate these computers by using Kerberos.
- Configure workgroup clients to use the Network Access Account so that these computers can retrieve content from distribution points.
- Provide an alternative mechanism for workgroup clients to find management points. Use DNS publishing, WINS, or directly assign a management point. These clients can't retrieve site information from Active Directory Domain Services.

For more information, see the following articles:

- Manage conflicting records
- Network access account
- How to install Configuration Manager clients on workgroup computers

Scenarios to support a site or hierarchy that spans multiple domains and forests

Scenario 1: Communication between sites in a hierarchy that spans forests

This scenario requires a two-way forest trust that supports Kerberos authentication. If you don't have a two-way forest trust that supports Kerberos authentication, then Configuration Manager doesn't support a child site in the remote forest.

Configuration Manager supports installing a child site in a remote forest that has the required two-way trust with the forest of the parent site. For example, you can place a secondary site in a different forest from its primary parent site as long as the required trust exists.

> **NOTE**
> A child site can be a primary site (where the central administration site is the parent site) or a secondary site.

Intersite communication in Configuration Manager uses database replication and file-based transfers. When you install a site, you must specify an account with which to install the site on the designated server. This account also establishes and maintains communication between sites. After the site successfully installs and initiates file-based transfers and database replication, you don't have to configure anything else for communication to the site.

When a two-way forest trust exists, Configuration Manager doesn't require any additional configuration steps.

By default, when you install a new child site, Configuration Manager configures the following components:

- An intersite file-based replication route at each site that uses the site server computer account. Configuration Manager adds the computer account of each computer to the **SMS_SiteToSiteConnection_<sitecode>** group on the destination computer.
- Database replication between the SQL Servers at each site.

Also set the following configurations:

- Intervening firewalls and network devices must allow the network packets that Configuration Manager requires.
- Name resolution must work between the forests.
- To install a site or site system role, you must specify an account that has local administrator permissions on the specified computer.

Scenario 2: Communication in a site that spans forests

This scenario doesn't require a two-way forest trust.

Primary sites support the installation of site system roles on computers in remote forests.

- The Application Catalog web service point is the only exception. It's only supported in the same forest as the site server.
- When a site system role accepts connections from the internet, as a security best practice, install the site system roles in a location where the forest boundary provides protection for the site server (for example, in a perimeter network).

To install a site system role on a computer in an untrusted forest:

- Specify a **Site System Installation Account**, which the site uses to install the site system role. (This account must have local administrative credentials to connect to.) Then install site system roles on the specified computer.
- Select the site system option **Require the site server to initiate connections to this site system**. This setting requires the site server to establish connections to the site system server to transfer data. This configuration prevents the computer in the untrusted location from initiating contact with the site server that's inside your trusted network. These connections use the **Site System Installation Account**.

To use a site system role that was installed in an untrusted forest, firewalls must allow the network traffic even when the site server initiates the transfer of data.

Additionally, the following site system roles require direct access to the site database. Therefore, firewalls must allow applicable traffic from the untrusted forest to the site's SQL Server:

- Asset Intelligence synchronization point

- Endpoint Protection point
- Enrollment point
- Management point
- Reporting service point
- State migration point

For more information, see Ports used in Configuration Manager.

You might need to configure the management point and enrollment point access to the site database.

- By default, when you install these roles, Configuration Manager configures the computer account of the new site system server as the connection account for the site system role. It then adds the account to the appropriate SQL Server database role.
- When you install these site system roles in an untrusted domain, configure the site system role connection account to enable the site system role to obtain information from the database.

If you configure a domain user account to be the connection account for these site system roles, make sure that the domain user account has appropriate access to the SQL Server database at that site:

- Management point: **Management Point Database Connection Account**
- Enrollment point: **Enrollment Point Connection Account**

Consider the following additional information when you plan for site system roles in other forests:

- If you run Windows Firewall, configure the applicable firewall profiles to pass communications between the site database server and computers that are installed with remote site system roles.
- When the internet-based management point trusts the forest that contains the user accounts, user policies are supported. When no trust exists, only computer policies are supported.

Scenario 3: Communication between clients and site system roles when the clients aren't in the same Active Directory forest as their site server

Configuration Manager supports the following scenarios for clients that aren't in the same forest as their site's site server:

- There's a two-way forest trust between the forest of the client and the forest of the site server.
- The site system role server is located in the same forest as the client.
- The client is on a domain computer that doesn't have a two-way forest trust with the site server, and site system roles aren't installed in the client's forest.
- The client is on a workgroup computer.

Clients on a domain-joined computer can use Active Directory Domain Services for service location when their site is published to their Active Directory forest.

To publish site information to another Active Directory forest:

- Specify the forest and then enable publishing to that forest in the **Active Directory Forests** node of the **Administration** workspace.
- Configure each site to publish its data to Active Directory Domain Services. This configuration enables clients in that forest to retrieve site information and find management points. For clients that can't use Active Directory Domain Services for service location, you can use DNS, WINS, or the client's assigned management point.

Scenario 4: Put the Exchange Server connector in a remote forest

To support this scenario, make sure that name resolution works between the forests. For example, configure DNS forwards. When you configure the Exchange Server connector, specify the intranet FQDN of the Exchange Server. For more information, see Manage mobile devices with Configuration Manager and Exchange.

See also

- Plan for security
- Security and privacy for Configuration Manager clients

Enhanced HTTP

8/28/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

> **TIP**
> This feature was first introduced in version 1806 as a pre-release feature. Beginning with version 1810, this feature is no longer a pre-release feature.

Microsoft recommends using HTTPS communication for all Configuration Manager communication paths, but it's challenging for some customers due to the overhead of managing PKI certificates.

Configuration Manager version 1806 includes improvements to how clients communicate with site systems. There are two primary goals for these improvements:

- You can secure sensitive client communication without the need for PKI server authentication certificates.
- Clients can securely access content from distribution points without the need for a network access account, client PKI certificate, and Windows authentication.

All other client communication is over HTTP. Enhanced HTTP isn't the same as enabling HTTPS for client communication or a site system.

> **NOTE**
> PKI certificates are still a valid option for customers with the following requirements:
>
> - All client communication is over HTTPS
> - Advanced control of the signing infrastructure

Scenarios

The following scenarios benefit from these improvements:

Scenario 1: Client to management point

Azure Active Directory (Azure AD)-joined devices can communicate with a management point configured for HTTP. The site server generates a certificate for the management point allowing it to communicate via a secure channel.

> **NOTE**
> This behavior is changed from Configuration Manager current branch version 1802, which requires an HTTPS-enabled management point for Azure AD-joined clients communicating through a cloud management gateway. For more information, see Enable management point for HTTPS.

Scenario 2: Client to distribution point

A workgroup or Azure AD-joined client can authenticate and download content over a secure channel from a distribution point configured for HTTP. These types of devices can also authenticate and download content from a distribution point configured for HTTPS without requiring a PKI certificate on the client. It's challenging to add a

client authentication certificate to a workgroup or Azure AD-joined client.

This behavior includes OS deployment scenarios with a task sequence running from boot media, PXE, or Software Center. For more information, see Network access account.

Scenario 3: Azure AD device identity

An Azure AD-joined or hybrid Azure AD device without an Azure AD user signed in can securely communicate with its assigned site. The cloud-based device identity is now sufficient to authenticate with the CMG and management point for device-centric scenarios. (A user token is still required for user-centric scenarios.)

Features

The following Configuration Manager features support or require enhanced HTTP:

- Cloud management gateway
- OS deployment without a network access account
- Enable co-management for new internet-based Windows 10 devices
- App approvals via email
- Administration service
- View recently connected consoles

> **NOTE**
> The software update point and related scenarios have always supported secure HTTP traffic with clients as well as the cloud management gateway. It uses a mechanism with the management point that's different from certificate- or token-based authentication.

Prerequisites

- A management point configured for HTTP client connections. Set this option on the **General** tab of the site system role properties.
- A distribution point configured for HTTP client connections. Set this option on the **General** tab of the site system role properties. Don't enable the option to **Allow clients to connect anonymously**.
- Onboard the site to Azure AD for cloud management.
  - If you've already met this prerequisite for your site, you need to update the Azure AD application. In the Configuration Manager console, go to the **Administration** workspace, expand **Cloud Services**, and select **Azure Active Directory Tenants**. Select the Azure AD tenant, select the web application in the **Applications** pane, and then select **Update application setting** in the ribbon.
- *For Scenario 3 only*: A client running Windows 10 version 1803 or later, and joined to Azure AD. The client requires this configuration for Azure AD device authentication.

Configure the site

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. Select the site and choose **Properties** in the ribbon.
2. Switch to the **Client Computer Communication** tab.

> **NOTE**
> Starting in version 1906, this tab is called **Communication Security**.

Select the option for **HTTPS or HTTP**. Then enable the option to **Use Configuration Manager-generated certificates for HTTP site systems**.

> **TIP**
> Wait up to 30 minutes for the management point to receive and configure the new certificate from the site.

Starting in version 1902, you can also enable enhanced HTTP for the central administration site. Use this same process, and open the properties of the central administration site. This action only enables enhanced HTTP for the SMS Provider roles at the central administration site. It's not a global setting that applies to all sites in the hierarchy.

You can see these certificates in the Configuration Manager console. Go to the **Administration** workspace, expand **Security**, and select the **Certificates** node. Look for the **SMS Issuing** root certificate, as well as the site server role certificates issued by the SMS Issuing root.

For more information on how the client communicates with the management point and distribution point with this configuration, see Communications from clients to site systems and services.

See also

- Plan for security
- Security and privacy for Configuration Manager clients
- Configure security
- Communication between endpoints

Hierarchy Maintenance Tool (Preinst.exe) for System Center Configuration Manager

5/9/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The Hierarchy Maintenance tool (Preinst.exe) passes commands to the System Center Configuration Manager Hierarchy Manager while the Hierarchy Manager service is running. The Hierarchy Maintenance tool is automatically installed when you install a Configuration Manager site. You can find Preinst.exe in the \\<*SiteServerName*>\SMS_<*SiteCode*>\bin\X64\00000409 shared folder on the site server.

You might use the Hierarchy Maintenance tool in the following scenarios:

- When secure key exchange is required, there are situations in which you must manually perform the initial public key exchange between sites. For more information, see Manually Exchange Public Keys Between Sites in this topic.
- To remove active jobs that are for a destination site that is no longer available.
- To delete a site server from the Configuration Manager console when you are unable to uninstall the site by using Setup. For example, if you physically remove a Configuration Manager site without first running Setup to uninstall the site, the site information will still exist in the parent site's database, and the parent site will continue to attempt to communicate with the child site. To resolve this issue, you must run the Hierarchy Maintenance tool and manually delete the child site from the parent site's database.
- To stop all Configuration Manager services at a site without having to stop services individually.
- When you are recovering a site, you can use the CHILDKEYS option to distribute the public keys from multiple child sites to the recovering site.

To run the Hierarchy Maintenance tool, the current user must have administrative privileges on the local computer. Also, the user must explicitly have the Site - Administer security right; it is not sufficient that the user inherits this right by being a member of a group that has that permission.

Hierarchy Maintenance Tool Command-Line Options

When you use the Hierarchy Maintenance Tool, you must run it locally on the central administration site, primary site, or secondary site server.

When you run the Hierarchy Maintenance tool, you must use the following syntax: preinst.exe /<option>. The following are the command-line options.

/DELJOB <*SiteCode*> - Use this option at a site to delete all jobs or commands from the current site to the specified destination site.

/DELSITE <*ChildSiteCodeToRemove*> - Use this option at a parent site to delete the data for child sites from the site database of the parent site. Typically, you use this option if a site server computer is decommissioned before you uninstall the site from it.

> **NOTE**
> The /DELSITE option does not uninstall the site on the computer specified by the ChildSiteCodeToRemove parameter. This option only removes the site information from the Configuration Manager site database.

/DUMP <*SiteCode*> - Use this option on the local site server to write site control images to the root folder of the drive on which the site is installed. You can write a specific site control image to the folder or write all site control files in the hierarchy.

- /DUMP <*SiteCode*> writes the site control image only for the specified site.
- /DUMP writes the site control files for all sites.

An image is a binary representation of the site control file, which is stored in the Configuration Manager site database. The dumped site control file image is a sum of the base image plus the pending delta images.

After dumping a site control file image with the Hierarchy Maintenance tool, the file name is in the format sitectrl_<*SiteCode*>.ct0.

/STOPSITE - Use this option on the local site server to initiate a shutdown cycle for the Configuration Manager Site Component Manager service, which partially resets the site. When this shutdown cycle is run, some Configuration Manager services on a site server and its remote site systems are stopped. These services are flagged for reinstallation. As a result of this shutdown cycle, some passwords are automatically changed when the services are reinstalled.

> **NOTE**
> If you want to see a record of shutdown, reinstallation, and password changes for Site Component Manager, enable logging for this component before using this command-line option.

After the shutdown cycle is started, it proceeds automatically, skipping any non-responding components or computers. However, if the Site Component Manager service cannot access a remote site system during the shutdown cycle, the components that are installed on the remote site system are reinstalled when the Site Component Manager service is restarted. When it is restarted, the Site Component Manager service repeatedly attempts reinstallation of all services that are flagged for reinstallation until it is successful.

You can restart the Site Component Manager service using Service Manager. After it is restarted, all affected services are uninstalled, reinstalled, and restarted. After you use the /STOPSITE option to initiate the shutdown cycle, you cannot avoid the reinstallation cycles after the Site Component Manager service is restarted.

/KEYFORPARENT - Use this option on a site to distribute the site's public key to a parent site.

The /KEYFORPARENT option places the public key of the site in the file <*SiteCode*>.CT4 at the root of the program files drive. After you run preinst.exe with this option, manually copy the <*SiteCode*>.CT4 file to the parent site's ...\Inboxes\hman.box folder (not hman.box\pubkey).

/KEYFORCHILD - Use this option on a site to distribute the site's public key to a child site.

The /KEYFORCHILD option places the public key of the site in the file <*SiteCode*>.CT5 at the root of the program files drive. After you run preinst.exe with this option, manually copy the <*SiteCode*>.CT5 file to the child site's ...\Inboxes\hman.box folder (not hman.box\pubkey).

/CHILDKEYS - You can use this option on the child sites of a site that you are recovering. Use this option to distribute public keys from multiple child sites to the recovering site.

The /CHILDKEYS option places the key from the site where you run the option, and all of that sites child sites public keys into the file <*SiteCode*>.CT6.

After you run preinst.exe with this option, manually copy the <*SiteCode*>.CT6 file to the recovering site's ...\Inboxes\hman.box folder (not hman.box\pubkey).

/PARENTKEYS - You can use this option on the parent site of a site that you are recovering. Use this option to distribute public keys from all parent sites to the recovering site.

The /PARENTKEYS option places the key from the site where you run the option, and the keys from each parent site above that site into the file <SiteCode>.CT7.

After you run preinst.exe with this option, manually copy the <*SiteCode*>.CT7 file to the recovering site's ...\Inboxes\hman.box folder (not hman.box\pubkey).

Manually Exchange Public Keys Between Sites

By default, the **Require secure key exchange** option is enabled for Configuration Manager sites. When secure key exchange is required, there are two situations in which you must manually perform the initial key exchange between sites:

- If the Active Directory schema has not been extended for Configuration Manager
- Configuration Manager sites are not publishing site data to Active Directory

You can use the Hierarchy Maintenance tool to export the public keys for each site. Once they have been exported, you must manually exchange the keys between the sites.

> **NOTE**
> After the public keys are manually exchanged, you can review the **hman.log** log file, which records site configuration changes and site information publication to Active Directory Domain Services, on the parent site server to ensure that the primary site has processed the new public key.

To manually transfer the child site public key to the parent site

1. While logged on to the child site, open a command prompt and navigate to the location of **Preinst.exe**.
2. Type the following to export the child site's public key: **Preinst /keyforparent**
3. The /keyforparent option places the public key of the child site in the **<site code>.CT4** file located at the root of the system drive.
4. Move the **<site code>.CT4** file to the parent site's **<install directory>\inboxes\hman.box** folder.

To manually transfer the parent site public key to the child site

1. While logged on to the parent site, open a command prompt and navigate to the location of **Preinst.exe**.
2. Type the following to export the parent site's public key: **Preinst /keyforchild**.
3. The /keyforchild option places the public key of the parent site in the **<site code>.CT5** file located at the root of the system drive.
4. Move the **<site code>.CT5** file to the **<install directory>\inboxes\hman.box** directory on the child site.

International support in System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The following sections provide technical details to help you make System Center Configuration Manager compliant with specific international requirements.

GB18030 Requirements

Configuration Manager meets the standards that are defined in GB18030 so that you can use Configuration Manager in China. A Configuration Manager deployment must have the following configurations to meet the GB18030 requirements:

- Each site server computer and SQL Server computer that you use with Configuration Manager must use a Chinese operating system.
- Each site database and each instance of SQL Server in the hierarchy must use the same collation, and must be one of the following:
  - Chinese_Simplified_Pinyin_100_CI_AI
  - Chinese_Simplified_Stroke_Order_100_CI_AI

  > **NOTE**
  > These database collations are an exception to the requirements that are noted in Support for SQL Server versions for System Center Configuration Manager.

- You must place a file with the name **GB18030.SMS** in the root folder of the system volume of each site server computer in the hierarchy. This file does not contain any data and can be an empty text file that is named to meet this requirement.

Interoperability between different versions of System Center Configuration Manager

5/29/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can install and operate multiple, independent hierarchies of System Center Configuration Manager on the same network. However, because different hierarchies of Configuration Manager don't interoperate outside of the migration process, each hierarchy requires configurations to prevent conflicts between them. Additionally, you can create certain configurations to help resources that you manage interact with the site systems from the correct hierarchy.

The following sections provide information about using different versions of Configuration Manager on the same network:

- Interoperability between System Center Configuration Manager and earlier product versions
- Interoperability for the Configuration Manager Console
- Configuration Manager limitations in a mixed-version hierarchy

Interoperability between System Center Configuration Manager and earlier product versions

Sites of different versions can't coexist in the same Configuration Manager hierarchy. The only exceptions are during the process of the following upgrade scenarios:

- From System Center 2012 Configuration Manager to System Center Configuration Manager
- From one System Center Configuration Manager version to a newer version using in-console updates

You can deploy a System Center Configuration Manager site and hierarchy side by side with an existing System Center 2012 Configuration Manager site or hierarchy. Plan to prevent clients from either version from trying to join a site from the other version.

For example, if two or more Configuration Manager hierarchies have overlapping boundaries that include the same network locations, assign each new client to a specific site instead of using automatic site assignment. For more information, see How to assign clients to a site.

Additionally, you can't install a client from System Center 2012 Configuration Manager on a computer that hosts a site system role from System Center Configuration Manager. You also can't you install a System Center Configuration Manager client on a computer that hosts a site system role from System Center 2012 Configuration Manager.

The following clients and connections aren't supported:

- Any System Center 2012 Configuration Manager or earlier computer client version
- Any System Center 2012 Configuration Manager or earlier device management client
- Windows CE Platform Builder device management client (any version)
- System Center Mobile Device Manager VPN connection

Client site assignment considerations

Configuration Manager clients can be assigned to only a single primary site. You can't predict the actual site assignment of a client when all of the following conditions are true:

- You use automatic site assignment to assign clients to a site during client installation
- More than one boundary group includes the same boundary
- The boundary groups have different assigned sites

If boundaries overlap across multiple Configuration Manager sites and hierarchies, clients might not be assigned to the site you expect, or might not get assigned to a site at all.

System Center Configuration Manager clients check the version of the site before they complete site assignment. If site boundaries overlap, you can't assign clients to a site with a previous version. However, earlier System Center 2012 Configuration Manager clients might incorrectly be assigned to a later System Center Configuration Manager site.

To prevent clients from unintentionally being assigned to the wrong site when two hierarchies have overlapping boundaries, configure client installation parameters to assign clients to a specific site.

Configuration Manager limitations in a mixed-version hierarchy

When you upgrade a System Center Configuration Manager hierarchy, there are times when different sites will have different versions. For example, first you upgrade the central administration site. Because of site maintenance windows, you don't upgrade the primary sites until a later time and date.

When different sites in a single hierarchy run different versions, some functionality isn't available. This behavior can affect how you manage Configuration Manager objects in the Configuration Manager console, and which functionality is available to clients. Typically, functionality from the newer version of Configuration Manager isn't accessible at sites or to clients that run a lower service pack version.

Network access account

You upgrade the central administration site to System Center Configuration Manager. You view the network access account details from a Configuration Manager console that's connected to this updated site. It doesn't display account details from sites that still run System Center 2012 Configuration Manager.

After you upgrade the primary site to the same version as the central administration site, the account details are visible in the console.

The same behavior applies when you update between versions of System Center Configuration Manager.

Boot images for OS deployment

When upgrading from System Center 2012 Configuration Manager to System Center Configuration Manager

When the top-level site of a hierarchy upgrades to System Center Configuration Manager, it automatically updates the default boot images to use the Windows Assessment and Deployment Kit (ADK) version 10. Use these boot images only for deployments to clients at System Center Configuration Manager sites. For more information, see Planning for OS deployment interoperability.

When upgrading between System Center Configuration Manager versions

As long as new versions of Configuration Manager don't update the version of Windows ADK that's in use, there's no effect on boot images.

New task sequence steps

When you create a task sequence with a step introduced in one version of Configuration Manager that's not available in an earlier version, you might have the following issues:

- An error occurs when you try to edit the task sequence from a site that's running a previous version of Configuration Manager.

- The task sequence doesn't run on a computer that runs a previous version of the Configuration Manager client.

Client to down-level management point communications

A Configuration Manager client that communicates with a management point from a site that runs a lower version than the client can only use functionality that the down-level version of Configuration Manager supports. For example, if you deploy content from a System Center Configuration Manager site that was recently upgraded to a client that communicates with a management point that hasn't yet upgraded to that version, that client can't use new functionality from the latest version.

Package and task sequence deployments to legacy clients

Starting in version 1902, you can't deploy a package or task sequence to a client version 5.7730 or earlier. To work around this limitation, upgrade the client to a later version.

Interoperability for the Configuration Manager console

This section contains information about the use of the Configuration Manager console in an environment that has a mix of Configuration Manager versions.

An environment with both System Center 2012 Configuration Manager and System Center Configuration Manager

To manage a Configuration Manager site, both the console and the site the console connects to must run the same version of Configuration Manager. For example, you can't use a System Center 2012 Configuration Manager console to manage a System Center Configuration Manager site, or the other way around.

It's not supported to install both the System Center 2012 Configuration Manager console and the System Center Configuration Manager console on the same computer.

An environment with multiple versions of System Center Configuration Manager

System Center Configuration Manager doesn't support installing more than a single Configuration Manager console on a computer. To use multiple consoles that are specific to different versions of System Center Configuration Manager, install the different consoles on separate computers.

During the process of updating sites in a hierarchy to a new version, you can connect a console to a site that runs a newer version and view information about other sites in that hierarchy. However, this configuration isn't recommended. It's possible that differences between the console version and Configuration Manager site version can result in data issues. Some features that are available in the latest product version won't be available in the console.

It's not supported to manage a site when using a console with a version that doesn't match the site version. Doing so might cause loss of data and can put your site at risk. For example, it's not supported to use a console from version 1610 to manage a site that runs version 1606.

Language packs in Configuration Manager

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article provides technical details about language support in Configuration Manager. Configuration Manager site servers and clients are considered language-neutral. Add support for display languages by installing **server language packs** or **client language packs** at a central administration site and at primary sites. You select the server and client languages to support at a site from the available language pack files during the site installation process.

Install multiple languages at each site. You only need to install the languages that you use.

- Each site supports multiple languages for Configuration Manager consoles.
- Add support for only the client languages that you want to support by installing individual client language packs at each site.

When you install support for a language that matches the following components:

- The display language of a computer: Both the Configuration Manager console and the client user interface that runs on that computer display information in that language.
- The language preference that is in use by the web browser of a computer: Connections to web-based information, including the Application Catalog or SQL Server Reporting Services, display in that language.

When you run Configuration Manager setup, it downloads language pack files as part of the prerequisites and redistributable files. You can also use the setup downloader to download these files before you run setup.

Server languages

Use the following table to map a locale ID to a language that you want to support on servers. For more information about locale IDs, see Locale IDs assigned by Microsoft.

SERVER LANGUAGE	LOCALE ID (LCID)	THREE-LETTER CODE
English (default)	0409	ENU
Chinese (Simplified)	0804	CHS
Chinese (Traditional, Taiwan)	0404	CHT
Czech	0405	CSY
Dutch - Netherlands	0413	NLD
French	040c	FRA
German	0407	DEU
Hungarian	040e	HUN

SERVER LANGUAGE	LOCALE ID (LCID)	THREE-LETTER CODE
Italian - Italy	0410	ITA
Japanese	0411	JPN
Korean	0412	KOR
Polish	0415	PLK
Portuguese - Brazil	0416	PTB
Portuguese - Portugal	0816	PTG
Russian	0419	RUS
Spanish - Spain	0c0a	ESN
Swedish	041d	SVE
Turkish	041f	TRK

Client languages

Use the following table to map a locale ID to a language that you want to support on client computers. For more information about locale IDs, see Locale IDs assigned by Microsoft.

CLIENT LANGUAGE	LOCALE ID (LCID)	THREE-LETTER CODE
English (default)	0409	ENG
Chinese -Simplified	0804	CHS
Chinese (Traditional, Taiwan)	0404	CHT
Czech	0405	CSY
Danish	0406	DAN
Dutch - Netherlands	0413	NLD
Finnish	040b	FIN
French	040c	FRA
German	0407	DEU
Greek	0408	ELL
Hungarian	040e	HUN
Italian - Italy	0410	ITA

CLIENT LANGUAGE	LOCALE ID (LCID)	THREE-LETTER CODE
Japanese	0411	JPN
Korean	0412	KOR
Norwegian	0414	NOR
Polish	0415	PLK
Portuguese (Brazil)	0416	PTB
Portuguese (Portugal)	0816	PTG
Russian	0419	RUS
Spanish - Spain	0c0a	ESN
Swedish	041d	SVE
Turkish	041f	TRK

Mobile device client languages

When you add support for mobile device languages, all supported mobile device client languages are included. You can't select individual language packs for mobile device support.

Identify installed language packs

To identify the language packs that are installed on a computer that runs the Configuration Manager client, look for the locale ID (LCID) of the installed language packs in the computer's registry. This information is available at the following registry path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCMSetup\InstalledLangs
```

Customize hardware inventory to collect this information. Then build a custom report to view the language details. For more information about collecting custom hardware inventory, see How to configure hardware inventory. For more information about creating reports, see Manage Configuration Manager reports.

About log files in Configuration Manager

7/26/2019 • 9 minutes to read • Edit Online

In Configuration Manager, client and site server components record process information in individual log files. You can use the information in these log files to help you troubleshoot issues that might occur. By default, Configuration Manager enables logging for client and server components.

This article provides general information about the Configuration Manager log files. It includes tools to use, how to configure the logs, and where to find them. For more information on specific log files, see Log files reference.

How it works

Most processes in Configuration Manager write operational information to a log file that is dedicated to that process. The log files are identified by **.log** or **.lo_** file extensions. Configuration Manager writes to a .log file until that log reaches its maximum size. When the log is full, the .log file is copied to a file of the same name but with the .lo_ extension, and the process or component continues to write to the .log file. When the .log file again reaches its maximum size, the .lo_ file is overwritten and the process repeats. Some components establish a log file history by appending a date and time stamp to the log file name and by keeping the .log extension.

Log viewer tools

All Configuration Manager log files are plain text, so you can view them with any text reader like Notepad. The logs use unique formatting that's best viewed with one of the following specialized tools:

- CMTrace
- OneTrace
- Support Center log viewer

CMTrace

To view the logs, use the Configuration Manager log viewer tool **CMTrace**. It's located in the \SMSSetup\Tools folder of the Configuration Manager source media. The CMTrace tool is added to all boot images that are added to the Software Library. Starting in version 1806, the CMTrace log viewing tool is automatically installed along with the Configuration Manager client. For more information, see CMTrace.

OneTrace

Starting in version 1906, **OneTrace** is a new log viewer with Support Center. It works similarly to CMTrace, with improvements. For more information, see Support Center OneTrace.

Support Center log viewer

Support Center includes a modern log viewer. This tool replaces CMTrace and provides a customizable interface with support for tabs and dockable windows. It has a fast presentation layer, and can load large log files in seconds. For more information, see Support Center Log Viewer reference.

> **NOTE**
> Support Center and OneTrace use Windows Presentation Foundation (WPF). This component isn't available in Windows PE. Continue to use CMTrace in boot images with task sequence deployments.

Configure logging options

You can change the configuration of the log files, such as the verbose level, size, and history. There are several ways to change these settings:

- During client installation
- Using Configuration Manager Service Manager
- Using the Windows Registry

Configure logging options during client installation

You can set the configuration of the client log files during installation. Use the following properties:

- CCMENABLELOGGING
- CCMDEBUGLOGGING
- CCMLOGLEVEL
- CCMLOGMAXHISTORY
- CCMLOGMAXSIZE

For more information, see Client installation properties.

Configure logging options by using Configuration Manager Service Manager

You can change where Configuration Manager stores the log files, and their size.

To modify the size of log files, change the name and location of the log file, or to force multiple components to write to a single log file, do the following steps:

Modify logging for a component

1. In the Configuration Manager console, go to the **Monitoring** workspace, expand **System Status**, and then select either the **Site Status** or **Component Status** node.
2. In the ribbon, select **Start**, and then select **Configuration Manager Service Manager**.
3. When Configuration Manager Service Manager opens, connect to the site that you want to manage. If the site that you want to manage isn't shown, select **Site**, select **Connect**, and then enter the name of the site server for the correct site.
4. Expand the site and go to **Components** or **Servers**, depending on where the components that you want to manage are located.
5. In the right pane, select one or more components.
6. On the **Component** menu, select **Logging**.
7. In the **Configuration Manager Component Logging** dialog box, complete the available configuration options for your selection.
8. Select **OK** to save the configuration.

Configure logging options by using the Windows Registry

Use the Windows Registry on the servers or clients to change the following logging options:

- Verbose level
- Maximum history
- Maximum size

When troubleshooting a problem, you can enable verbose logging for Configuration Manager to write additional details in the log files.

> **WARNING**
> Misconfiguration of these settings can cause Configuration Manager to log large amounts of information, or none at all. While this data can be beneficial for troubleshooting, be cautious when changing these values in production sites. Always test these changes in a lab environment first. Excessive logging can occur, which might make it difficult to find relevant information in the log files.

After you make changes to these registry settings, restart the component:

- If you change the client settings, restart the **SMS Agent Host** service (CcmExec).
- If you change the server settings, restart the **SMS Executive** service.

The registry settings vary depending upon the component:

- Client and management point
- Site server
- Site system role
- Configuration Manager console

Client and management point logging options

To configure logging options for all components on a client or management point site system, configure these **REG_DWORD** values under the following Windows Registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM\Logging\@Global`

NAME	VALUES	DESCRIPTION
LogLevel	`0`: Verbose `1`: Default `2`: Warnings and errors `3`: Errors only	The level of detail to write to log files.
LogMaxHistory	Any integer greater than or equal to zero, for example: `0`: No history `1`: Default	When a log file reaches the maximum size, the client renames it as a backup and creates a new log file. Specify how many previous versions to keep.
LogMaxSize	Any integer greater than or equal to 10,000, for example: 250000	The maximum log file size in bytes. When a log grows to the specified size, the client renames it as a history file, and creates a new file. The default value is 250,000 bytes.

> **NOTE**
> Don't change other values that may exist in this registry key.

For advanced debugging, you can also add this **REG_SZ** value under the following Windows Registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM\Logging\DebugLogging`

NAME	VALUES	DESCRIPTION
Enabled	`True`: enable debug logs `False`: disable debug logs	Enables debug logging for troubleshooting purposes.

NAME	VALUES	DESCRIPTION

This setting causes the client to log low-level information for troubleshooting. Avoid using this setting in production sites. Excessive logging can occur, which might make it difficult to find relevant information in the log files. Make sure to turn off this setting after you resolve the issue.

Site server logging options

You can configure settings globally or for a specific component on the Configuration Manager site server.

Configure these values under the following Windows Registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Tracing`

NAME	VALUES	TYPE	DESCRIPTION
SqlEnabled	`1`: enable SQL tracing `0`: disable SQL tracing	REG_DWORD	Add SQL trace logging to all site server logs.
ArchiveEnabled	`1`: enable log archives `0`: disable log archives	REG_DWORD	Archive site server logs to a separate location for historical preservation.
ArchivePath	A valid folder path, for example `C:\Logs\Archive`	REG_SZ	The path to archive site server logs.

Only enable SQL tracing for troubleshooting purposes. Avoid using it in production sites. Excessive logging can occur, which might make it difficult to find relevant information in the log files. Make sure to turn off this setting after you resolve the issue.

> **NOTE**
> Don't change other values that may exist in this registry key.

To configure logging options for a specific server component, configure these **REG_DWORD** values under the following Windows Registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Tracing\<ComponentName>`

NAME	VALUES	DESCRIPTION
LoggingLevel	`0`: Verbose `1`: Default `2`: Warnings and errors `3`: Errors only	The level of detail to write to log files.
LogMaxHistory	Any integer greater than or equal to zero, for example: `0`: No history `1`: Default	When a log file reaches the maximum size, the server renames it as a backup and creates a new log file. Specify how many previous versions to keep.

NAME	VALUES	DESCRIPTION
MaxFileSize	Any integer greater than or equal to 10,000, for example: 250000	The maximum log file size in bytes. When a log grows to the specified size, the client renames it as a history file, and creates a new file. The default value is 250,000 bytes.
DebugLogging	`1`: enable debug logs `0`: disable debug logs	Enables debug logging for troubleshooting purposes.

The DebugLogging setting causes the server to log low-level information for troubleshooting. Avoid using this setting in production sites. Excessive logging can occur, which might make it difficult to find relevant information in the log files. Make sure to turn off this setting after you resolve the issue.

> **NOTE**
> Don't change other values that may exist in this registry key.

Site system role logging options

You can configure settings globally or for a specific component on a site system that hosts a Configuration Manager server role.

To configure logging options for a specific server component, configure these **REG_DWORD** values under the following Windows Registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\<ComponentName>\Logging
```

For example, for the distribution point role:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\DP\Logging
```

NAME	VALUES	DESCRIPTION
LogLevel	`0`: Verbose `1`: Default `2`: Warnings and errors `3`: Errors only	The level of detail to write to log files.
LogMaxHistory	Any integer greater than or equal to zero, for example: `0`: No history `1`: Default	When a log file reaches the maximum size, the server renames it as a backup and creates a new log file. Specify how many previous versions to keep.
LogMaxSize	Any integer greater than or equal to 10,000, for example: 250000	The maximum log file size in bytes. When a log grows to the specified size, the server renames it as a history file, and creates a new file. The default value is 250,000 bytes.

> **NOTE**
> Don't change other values that may exist in this registry key.

Configuration Manager console logging options

To change the verbose level of the AdminUI.log for the Configuration Manager console, use the following

procedure:

1. Open the console configuration file, **Microsoft.ConfigurationManagement.exe.config**, in an XML editor like Notepad. The default configuration file is in the following location:
   ```
   C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\bin\Microsoft.ConfigurationManagement.exe.config
   ```
2. Under the **system.diagnostics** > **sources** > **source** element, change the **switchValue** attribute from `Error` to `Verbose`. For example:

   Original: `<source name="SmsAdminUISnapIn" switchValue="Error">` New:
   `<source name="SmsAdminUISnapIn" switchValue="Verbose" >`
3. Save the file, and restart the console.

Locating log files

Configuration Manager and dependent components store log files in various locations. These locations depend on the process that creates the log file and the configuration of your environment.

The following locations are the defaults. If you customized the installation directories in your environment, the actual paths may vary.

- Client: `C:\Windows\CCM\logs`
- Server: `C:\Program Files\Microsoft Configuration Manager\Logs`
- Management point: `C:\SMS_CCM\Logs`
- Configuration Manager console: `C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\AdminUILog`
- IIS: `C:\inetpub\logs\logfiles\w3svc1`

Task sequence log locations

The location of the task sequence log file **smsts.log** varies depending upon the phase of the task sequence:

- In Windows PE before Format and Partition Disk step: `X:\Windows\temp\smstslog\smsts.log` (X is the Windows PE RAM drive)
- In Windows PE after **Format and Partition Disk** step: `X:\smstslog\smsts.log`, then copied to `C:\_SMSTaskSequence\Logs\smstslog\smsts.log` when drive is ready
- In the new Windows OS before the client is installed: `C:\_SMSTaskSequence\Logs\smstslog\smsts.log`
- In Windows after the client is installed: `C:\Windows\CCM\Logs\smstslog\smsts.log`
- In Windows after the task sequence completes: `C:\Windows\CCM\Logs\smsts.log`

> **TIP**
> The read-only task sequence variable _SMSTSLogPath always contains the path of the current log file.

See also

- Log files reference
- Support Center OneTrace
- Support Center log file viewer
- CMTrace

Log file reference

9/4/2019 • 45 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

In Configuration Manager, client and site server components record process information in individual log files. You can use the information in these log files to help you troubleshoot issues that might occur. By default, Configuration Manager enables logging for client and server components.

For more general information about log files in Configuration Manager, see About log files. That article includes information on the tools to use, how to configure the logs, and where to find them.

The following sections provide details about the different log files available to you. Monitor Configuration Manager client and server logs for operation details, and view error information to troubleshoot problems.

- Content management
- Desktop Analytics
- Discovery
- Endpoint Protection
- Extensions
- Inventory
- Migration
- Mobile devices
- OS deployment
- Power management
- Remote control
- Reporting
- Role-based administration
- Software metering
- Software updates
- Wake On LAN
- Windows 10 servicing
- Windows Update Agent
- WSUS server

Client log files

The following sections list the log files related to client operations and client installation.

Client operations

The following table lists the log files located on the Configuration Manager client.

LOG NAME	DESCRIPTION
CAS.log	The Content Access service. Maintains the local package cache on the client.
Ccm32BitLauncher.log	Records actions for starting applications on the client marked *run as 32 bit*.
CcmEval.log	Records Configuration Manager client status evaluation activities and details for components that are required by the Configuration Manager client.
CcmEvalTask.log	Records the Configuration Manager client status evaluation activities that are initiated by the evaluation scheduled task.

LOG NAME	DESCRIPTION
CcmExec.log	Records activities of the client and the SMS Agent Host service. This log file also includes information about enabling and disabling wake-up proxy.
CcmMessaging.log	Records activities related to communication between the client and management points.
CCMNotificationAgent.log	Records activities related to client notification operations.
Ccmperf.log	Records activities related to the maintenance and capture of data related to client performance counters.
CcmRestart.log	Records client service restart activity.
CCMSDKProvider.log	Records activities for the client SDK interfaces.
CertificateMaintenance.log	Maintains certificates for Active Directory Domain Services and management points.
CIDownloader.log	Records details about configuration item definition downloads.
CITaskMgr.log	Records tasks that are initiated for each application and deployment type, such as content download and install or uninstall actions.
ClientAuth.log	Records signing and authentication activity for the client.
ClientIDManagerStartup.log	Creates and maintains the client GUID and identifies tasks performed during client registration and assignment.
ClientLocation.log	Records tasks that are related to client site assignment.
CMHttpsReadiness.log	Records the results of running the Configuration Manager HTTPS Readiness Assessment Tool. This tool checks whether computers have a public key infrastructure (PKI) client authentication certificate that can be used with Configuration Manager.
CmRcService.log	Records information for the remote control service.
CoManagementHandler.log	Use to troubleshoot co-management on the client.
ContentTransferManager.log	Schedules the Background Intelligent Transfer Service (BITS) or Server Message Block (SMB) to download or access packages.
DataTransferService.log	Records all BITS communication for policy or package access.
DeltaDownload.log	Records information about the download of express updates and updates downloaded using Delivery Optimization.
EndpointProtectionAgent	Records information about the installation of the System Center Endpoint Protection client and the application of antimalware policy to that client.

LOG NAME	DESCRIPTION
execmgr.log	Records details about packages and task sequences that run on the client.
ExpressionSolver.log	Records details about enhanced detection methods that are used when verbose or debug logging is turned on.
ExternalEventAgent.log	Records the history of Endpoint Protection malware detection and events related to client status.
FileBITS.log	Records all SMB package access tasks.
FileSystemFile.log	Records the activity of the Windows Management Instrumentation (WMI) provider for software inventory and file collection.
FSPStateMessage.log	Records the activity for state messages that are sent to the fallback status point by the client.
InternetProxy.log	Records the network proxy configuration and use activity for the client.
InventoryAgent.log	Records activities of hardware inventory, software inventory, and heartbeat discovery actions on the client.
LocationCache.log	Records the activity for location cache use and maintenance for the client.
LocationServices.log	Records the client activity for locating management points, software update points, and distribution points.
M365AHandler.log	Information about the Desktop Analytics settings policy
MaintenanceCoordinator.log	Records the activity for general maintenance tasks for the client.
Mifprovider.log	Records the activity of the WMI provider for Management Information Format (MIF) files.
mtrmgr.log	Monitors all software metering processes.
PolicyAgent.log	Records requests for policies made by using the Data Transfer Service.
PolicyAgentProvider.log	Records policy changes.
PolicyEvaluator.log	Records details about the evaluation of policies on client computers, including policies from software updates.
PolicyPlatformClient.log	Records the process of remediation and compliance for all providers located in \Program Files\Microsoft Policy Platform, except the file provider.
PolicySdk.log	Records activities for policy system SDK interfaces.

LOG NAME	DESCRIPTION
Pwrmgmt.log	Records information about enabling or disabling and configuring the wake-up proxy client settings.
PwrProvider.log	Records the activities of the power management provider (PWRInvProvider) hosted in the WMI service. On all supported versions of Windows, the provider enumerates the current settings on computers during hardware inventory and applies power plan settings.
SCClient_<*domain*>@<*username*>_1.log	Records the activity in Software Center for the specified user on the client computer.
SCClient_<*domain*>@<*username*>_2.log	Records the historical activity in Software Center for the specified user on the client computer.
Scheduler.log	Records activities of scheduled tasks for all client operations.
SCNotify_<*domain*>@<*username*>_1.log	Records the activity for notifying users about software for the specified user.
SCNotify_<*domain*>@<*username*>_1-<*date_time*>.log	Records the historical information for notifying users about software for the specified user.
setuppolicyevaluator.log	Records configuration and inventory policy creation in WMI.
SleepAgent_<*domain*>@SYSTEM_0.log	The main log file for wake-up proxy.
smscliui.log	Records use of the Configuration Manager client in Control Panel.
SrcUpdateMgr.log	Records activity for installed Windows Installer applications that are updated with current distribution point source locations.
StatusAgent.log	Records status messages that are created by the client components.
SWMTRReportGen.log	Generates a use data report that is collected by the metering agent. This data is logged in Mtrmgr.log.
UserAffinity.log	Records details about user device affinity.
VirtualApp.log	Records information specific to the evaluation of Application Virtualization (App-V) deployment types.
Wedmtrace.log	Records operations related to write filters on Windows Embedded clients.
wakeprxy-install.log	Records installation information when clients receive the client setting option to turn on wake-up proxy.
wakeprxy-uninstall.log	Records information about uninstalling wake-up proxy when clients receive the client setting option to turn off wake-up proxy, if wake-up proxy was previously turned on.

Client installation

The following table lists the log files that contain information related to the installation of the Configuration Manager client.

LOG NAME	DESCRIPTION
ccmsetup.log	Records ccmsetup.exe tasks for client setup, client upgrade, and client removal. Can be used to troubleshoot client installation problems.
ccmsetup-ccmeval.log	Records ccmsetup.exe tasks for client status and remediation.
CcmRepair.log	Records the repair activities of the client agent.
client.msi.log	Records setup tasks performed by client.msi. Can be used to troubleshoot client installation or removal problems.

Client for Linux and UNIX

> **IMPORTANT**
> Starting in version 1902, Configuration Manager doesn't support Linux or UNIX clients.
>
> Consider Microsoft Azure Management for managing Linux servers. Azure solutions have extensive Linux support that in most cases exceed Configuration Manager functionality, including end-to-end patch management for Linux.

The Configuration Manager client for Linux and UNIX records information in the following log files:

> **TIP**
> Use CMTrace to view the log files for the client for Linux and UNIX.

LOG NAME	DETAILS
Scxcm.log	The log file for the core service of the Configuration Manager client for Linux and UNIX (ccmexec.bin). This log file contains information about the installation and ongoing operations of ccmexec.bin. By default, this log file is located at **/var/opt/microsoft/scxcm.log** To change the location of the log file, edit **/opt/microsoft/configmgr/etc/scxcm.conf** and change the **PATH** field. You don't need to restart the client computer or service for the change to take effect. You can set the log level to one of four different settings.

LOG NAME	DETAILS
Scxcmprovider.log	The log file for the CIM service of the Configuration Manager client for Linux and UNIX (omiserver.bin). This log file contains information about the ongoing operations of nwserver.bin. This log is located at**/var/opt/microsoft/configmgr/scxcmprovider.log** To change the location of the log file, edit **/opt/microsoft/omi/etc/scxcmprovider.conf** and change the **PATH** field. You don't need to restart the client computer or service for the change to take effect. You can set the log level to one of three settings.

Both log files support several levels of logging:

- **scxcm.log**. To change the log level, edit **/opt/microsoft/configmgr/etc/scxcm.conf** and change each instance of the **MODULE** tag to the log level you want:
  - ERROR: Indicates problems that require attention
  - WARNING: Indicates possible problems for client operations
  - INFO: More detailed logging that indicates the status of various events on the client
  - TRACE: Verbose logging that typically is used to diagnose problems
- **scxcmprovider.log**. To change the log level, edit **/opt/microsoft/omi/etc/scxcmprovider.conf** and change each instance of the **MODULE** tag to the log level you want:
  - ERROR: Indicates problems that require attention
  - WARNING: Indicates possible problems for client operations
  - INFO: More detailed logging that indicates the status of various events on the client

Under normal operating conditions, use the ERROR log level. This log level creates the smallest log file. As the log level is increased from ERROR to WARNING, to INFO, and then to TRACE, a larger log file is created as more data is written to the file.

Manage log files for the Linux and UNIX client

The client for Linux and UNIX doesn't limit the maximum size of the client log files. It also doesn't automatically copy the contents of its .log files to another file, such as to a .lo_ file. If you want to control the maximum size of log files, implement a process to manage the log files independent from the Configuration Manager client for Linux and UNIX.

For example, you can use the standard Linux and UNIX command **logrotate** to manage the size and rotation of the client log files. The Configuration Manager client for Linux and UNIX has an interface that enables **logrotate** to signal the client when the log rotation completes, so the client can resume logging to the log file.

For information about **logrotate**, see the documentation for the Linux and UNIX distributions that you use.

Client for Mac computers

The Configuration Manager client for Mac computers records information in the following log files:

LOG NAME	DETAILS

LOG NAME	DETAILS
CCMClient-<*date_time*>.log	Records activities that are related to the Mac client operations, including application management, inventory, and error logging. This log file is located in the /Library/Application Support/Microsoft/CCM/Logs folder on the Mac computer.
CCMAgent-<*date_time*>.log	Records information that is related to client operations, including user sign in and sign out operations, and Mac computer activity. This log file is in the ~/Library/Logs folder on the Mac computer.
CCMNotifications-<*date_time*>.log	Records activities that are related to Configuration Manager notifications displayed on the Mac computer. This log file is located in the ~/Library/Logs folder on the Mac computer.
CCMPrefPane-<*date_time*>.log	Records activities related to the Configuration Manager preferences dialog box on the Mac computer, which includes general status and error logging. This log file is located in the ~/Library/Logs folder on the Mac computer.

The log file **SMS_DM.log** on the site system server also records communication between Mac computers and the management point that is set up for mobile devices and Mac computers.

Server log files

The following sections list log files that are on the site server or that are related to specific site system roles.

Site server and site systems

The following table lists the log files that are on the Configuration Manager site server and site system servers.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
adctrl.log	Records enrollment processing activity.	Site server
ADForestDisc.log	Records Active Directory Forest Discovery actions.	Site server
adminservice.log	Records actions for the SMS Provider administration service REST API	Computer with the SMS Provider
ADService.log	Records account creation and security group details in Active Directory.	Site server
adsgdis.log	Records Active Directory Group Discovery actions.	Site server
adsysdis.log	Records Active Directory System Discovery actions.	Site server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
adusrdis.log	Records Active Directory User Discovery actions.	Site server
BusinessAppProcessWorker.log	Records processing for Microsoft Store for Business apps.	Site server
ccm.log	Records activities for client push installation.	Site server
CertMgr.log	Records certificate activities for intrasite communication.	Site system server
chmgr.log	Records activities of the client health manager.	Site server
Cidm.log	Records changes to the client settings by the Client Install Data Manager (CIDM).	Site server
colleval.log	Records details about when collections are created, changed, and deleted by the Collection Evaluator.	Site server
compmon.log	Records the status of component threads monitored for the site server.	Site system server
compsumm.log	Records Component Status Summarizer tasks.	Site server
ComRegSetup.log	Records the initial installation of COM registration results for a site server.	Site system server
dataldr.log	Records information about the processing of MIF files and hardware inventory in the Configuration Manager database.	Site server
ddm.log	Records activities of the discovery data manager.	Site server
despool.log	Records incoming site-to-site communication transfers.	Site server
distmgr.log	Records details about package creation, compression, delta replication, and information updates.	Site server
EPCtrlMgr.log	Records information about the syncing of malware threat information from the Endpoint Protection site system role server with the Configuration Manager database.	Site server
EPMgr.log	Records the status of the Endpoint Protection site system role.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
EPSetup.log	Provides information about the installation of the Endpoint Protection site system role.	Site system server
EnrollSrv.log	Records activities of the enrollment service process.	Site system server
EnrollWeb.log	Records activities of the enrollment website process.	Site system server
fspmgr.log	Records activities of the fallback status point site system role.	Site system server
hman.log	Records information about site configuration changes, and about the publishing of site information in Active Directory Domain Services.	Site server
Inboxast.log	Records the files that are moved from the management point to the corresponding INBOXES folder on the site server.	Site server
inboxmgr.log	Records file transfer activities between inbox folders.	Site server
inboxmon.log	Records the processing of inbox files and performance counter updates.	Site server
invproc.log	Records the forwarding of MIF files from a secondary site to its parent site.	Site server
migmctrl.log	Records information for Migration actions that involve migration jobs, shared distribution points, and distribution point upgrades.	Top-level site in the Configuration Manager hierarchy, and each child primary site. In a multi-primary site hierarchy, use the log file that is created at the central administration site.
mpcontrol.log	Records the registration of the management point with Windows Internet Name Service (WINS). Records the availability of the management point every 10 minutes.	Site system server
mpfdm.log	Records the actions of the management point component that moves client files to the corresponding INBOXES folder on the site server.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
mpMSI.log	Records details about the management point installation.	Site server
MPSetup.log	Records the management point installation wrapper process.	Site server
netdisc.log	Records Network Discovery actions.	Site server
NotiCtrl.log	Application request notifications.	Site server
ntsvrdis.log	Records the discovery activity of site system servers.	Site server
Objreplmgr	Records the processing of object change notifications for replication.	Site server
offermgr.log	Records advertisement updates.	Site server
offersum.log	Records the summarization of deployment status messages.	Site server
OfflineServicingMgr.log	Records the activities of applying updates to operating system image files.	Site server
outboxmon.log	Records the processing of outbox files and performance counter updates.	Site server
PerfSetup.log	Records the results of the installation of performance counters.	Site system server
PkgXferMgr.log	Records the actions of the SMS_Executive component that is responsible for sending content from a primary site to a remote distribution point.	Site server
policypv.log	Records updates to the client policies to reflect changes to client settings or deployments.	Primary site server
rcmctrl.log	Records the activities of database replication between sites in the hierarchy.	Site server
replmgr.log	Records the replication of files between the site server components and the Scheduler component.	Site server
ResourceExplorer.log	Records errors, warnings, and information about running Resource Explorer.	Computer that runs the Configuration Manager console

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
ruleengine.log	Records details about automatic deployment rules for the identification, content download, and software update group and deployment creation.	Site server
schedule.log	Records details about site-to-site job and file replication.	Site server
sender.log	Records the files that transfer by file-based replication between sites.	Site server
sinvproc.log	Records information about the processing of software inventory data to the site database.	Site server
sitecomp.log	Records details about the maintenance of the installed site components on all site system servers in the site.	Site server
sitectrl.log	Records site setting changes made to site control objects in the database.	Site server
sitestat.log	Records the availability and disk space monitoring process of all site systems.	Site server
SMS_AZUREAD_DISCOVERY_AGENT.log	Log file for synchronization of collection membership results to Azure Active directory. This was first introduced as a pre-release feature starting in Configuration Manager version 1906.	Site server
SMS_BUSINESS_APP_PROCESS_MANAGER.log	Log file for component that synchronizes apps from the Microsoft Store for Business.	Site server
SMS_ISVUPDATES_SYNCAGENT.log	Log file for synchronization of third-party software updates starting in Configuration Manager version 1806.	Top-level software update point in the Configuration Manager hierarchy.
SMS_PhasedDeployment.log	Log file for phased deployments	Top-level site in the Configuration Manager hierarchy
SmsAdminUI.log	Records Configuration Manager console activity.	Computer that runs the Configuration Manager console
SMSAWEBSVCSetup.log	Records the installation activities of the Application Catalog web service.	Site system server
smsbkup.log	Records output from the site backup process.	Site server
smsdbmon.log	Records database changes.	Site server
SMSENROLLSRVSetup.log	Records the installation activities of the enrollment web service.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
SMSENROLLWEBSetup.log	Records the installation activities of the enrollment website.	Site system server
smsexec.log	Records the processing of all site server component threads.	Site server or site system server
SMSFSPSetup.log	Records messages generated by the installation of a fallback status point.	Site system server
SMSPORTALWEBSetup.log	Records the installation activities of the Application Catalog website.	Site system server
SMSProv.log	Records WMI provider access to the site database.	Computer with the SMS Provider
srsrpMSI.log	Records detailed results of the reporting point installation process from the MSI output.	Site system server
srsrpsetup.log	Records results of the reporting point installation process.	Site system server
statesys.log	Records the processing of state system messages.	Site server
statmgr.log	Records the writing of all status messages to the database.	Site server
swmproc.log	Records the processing of metering files and settings.	Site server

Site server installation

The following table lists the log files that contain information related to site installation.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
ConfigMgrPrereq.log	Records prerequisite component evaluation and installation activities.	Site server
ConfigMgrSetup.log	Records detailed output from the site server setup.	Site Server
ConfigMgrSetupWizard.log	Records information related to activity in the Setup Wizard.	Site Server
SMS_BOOTSTRAP.log	Records information about the progress of launching the secondary site installation process. Details of the actual setup process are contained in ConfigMgrSetup.log.	Site Server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
smstsvc.log	Records information about the installation, use, and removal of a Windows service that is used to test network connectivity and permissions between servers, using the computer account of the server that initiates the connection.	Site server and site system server

Data warehouse service point

The following table lists the log files that contain information related to the data warehouse service point.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
DWSSMSI.log	Records messages generated by the installation of a data warehouse service point.	Site system server
DWSSSetup.log	Records messages generated by the installation of a data warehouse service point.	Site system server
Microsoft.ConfigMgrDataWarehouse.log	Records information about data synchronization between the site database and the data warehouse database.	Site system server

Fallback status point

The following table lists the log files that contain information related to the fallback status point.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
FspIsapi	Records details about communications to the fallback status point from mobile device legacy clients and client computers.	Site system server
fspMSI.log	Records messages generated by the installation of a fallback status point.	Site system server
fspmgr.log	Records activities of the fallback status point site system role.	Site system server

Management point

The following table lists the log files that contain information related to the management point.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
CcmIsapi.log	Records client messaging activity on the endpoint.	Site system server
MP_CliReg.log	Records the client registration activity processed by the management point.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
MP_Ddr.log	Records the conversion of XML.ddr records from clients, and then copies them to the site server.	Site system server
MP_Framework.log	Records the activities of the core management point and client framework components.	Site system server
MP_GetAuth.log	Records client authorization activity.	Site system server
MP_GetPolicy.log	Records policy request activity from client computers.	Site system server
MP_Hinv.log	Records details about the conversion of XML hardware inventory records from clients and the copy of those files to the site server.	Site system server
MP_Location.log	Records location request and reply activity from clients.	Site system server
MP_OOBMgr.log	Records the management point activities related to receiving an OTP from a client.	Site system server
MP_Policy.log	Records policy communication.	Site system server
MP_Relay.log	Records the transfer of files that are collected from the client.	Site system server
MP_Retry.log	Records hardware inventory retry processes.	Site system server
MP_Sinv.log	Records details about the conversion of XML software inventory records from clients and the copy of those files to the site server.	Site system server
MP_SinvCollFile.log	Records details about file collection.	Site system server
MP_Status.log	Records details about the conversion of XML.svf status message files from clients and the copy of those files to the site server.	Site system server
mpcontrol.log	Records the registration of the management point with WINS. Records the availability of the management point every 10 minutes.	Site server
mpfdm.log	Records the actions of the management point component that moves client files to the corresponding INBOXES folder on the site server.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
mpMSI.log	Records details about the management point installation.	Site server
MPSetup.log	Records the management point installation wrapper process.	Site server
UserService.log	Records user requests from Software Center, retrieving/installing user-available applications from the server.	Site system server

Service connection point

The following table lists the log files that contain information related to the service connection point.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
CertMgr.log	Records certificate and proxy account information.	Site server
CollEval.log	Records details about when collections are created, changed, and deleted by the Collection Evaluator.	Primary site and central administration site
Cloudusersync.log	Records license enablement for users.	Computer with the service connection point
Dataldr.log	Records information about the processing of MIF files.	Site server
ddm.log	Records activities of the discovery data manager.	Site server
Distmgr.log	Records details about content distribution requests.	Top-level site server
Dmpdownloader.log	Records details about downloads from Microsoft Intune.	Computer with the service connection point
Dmpuploader.log	Records detail related to uploading database changes to Microsoft Intune.	Computer with the service connection point
hman.log	Records information about message forwarding.	Site server
MSfBSyncWorker.log	Records information about the communication with the Microsoft Store for Business.	Computer with the service connection point
objreplmgr.log	Records the processing of policy and assignment.	Primary site server
PolicyPV.log	Records policy generation of all policies.	Site server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
outgoingcontentmanager.log	Records content uploaded to Microsoft Intune.	Computer with the service connection point
Sitecomp.log	Records details of service connection point installation.	Site server
SmsAdminUI.log	Records Configuration Manager console activity.	Computer that runs the Configuration Manager console
SMS_CLOUDCONNECTION.log	Records information about cloud services.	Computer with the service connection point
Smsprov.log	Records activities performed by the SMS Provider. Configuration Manager console activities use the SMS Provider.	Computer with the SMS Provider
SrvBoot.log	Records details about the service connection point installer service.	Computer with the service connection point
Statesys.log	Records the processing of mobile device management messages.	Primary site and central administration site

Software update point

The following table lists the log files that contain information related to the software update point.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
objreplmgr.log	Records details about the replication of software updates notification files from a parent site to child sites.	Site server
PatchDownloader.log	Records details about the process of downloading software updates from the update source to the download destination on the site server.	When you manually download updates, this file is in your `%temp%` directory on the computer where you use the console. For automatic deployment rules, if the Configuration Manager client is installed on the site server, this file is on the site server in `%windir%\CCM\Logs`.
ruleengine.log	Records details about automatic deployment rules for the identification, content download, and software update group and deployment creation.	Site server
SMS_ISVUPDATES_SYNCAGENT.log	Log file for synchronization of third-party software updates starting in Configuration Manager version 1806.	Top-level software update point in the Configuration Manager hierarchy.
SUPSetup.log	Records details about the software update point installation. When the software update point installation completes, **Installation was successful** is written to this log file.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
WCM.log	Records details about the software update point configuration and connections to the WSUS server for subscribed update categories, classifications, and languages.	Site server that connects to the WSUS server
WSUSCtrl.log	Records details about the configuration, database connectivity, and health of the WSUS server for the site.	Site system server
wsyncmgr.log	Records details about the software updates sync process.	Site system server
WUSSyncXML.log	Records details about the Inventory Tool for the Microsoft Updates sync process.	Client computer configured as the sync host for the Inventory Tool for Microsoft Updates

Log files by functionality

The following sections list log files related to Configuration Manager functions.

Application management

The following table lists the log files that contain information related to application management.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
AppIntentEval.log	Records details about the current and intended state of applications, their applicability, whether requirements were met, deployment types, and dependencies.	Client
AppDiscovery.log	Records details about the discovery or detection of applications on client computers.	Client
AppEnforce.log	Records details about enforcement actions (install and uninstall) taken for applications on the client.	Client
AppGroupHandler.log	Starting in version 1906, detection and enforcement information for application groups	Client
awebsctl.log	Records monitoring activities for the Application Catalog web service point site system role.	Site system server
awebsvcMSI.log	Records detailed installation information for the Application Catalog web service point site system role.	Site system server
BusinessAppProcessWorker.log	Records processing for Microsoft Store for Business apps.	Site server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
Ccmsdkprovider.log	Records the activities of the application management SDK.	Client
colleval.log	Records details about when collections are created, changed, and deleted by the Collection Evaluator.	Site system server
ConfigMgrSoftwareCatalog.log	Records the activity of the Application Catalog, which includes its use of Silverlight.	Client
MSfBSyncWorker.log	Records information about the communication with the Microsoft Store for Business.	Computer with the service connection point
NotiCtrl.log	Application request notifications.	Site server
portlctl.log	Records the monitoring activities for the Application Catalog website point site system role.	Site system server
portlwebMSI.log	Records the MSI installation activity for the Application Catalog website role.	Site system server
PrestageContent.log	Records details about the use of the ExtractContent.exe tool on a remote, prestaged distribution point. This tool extracts content that has been exported to a file.	Site system server
ServicePortalWebService.log	Records the activity of the Application Catalog web service.	Site system server
ServicePortalWebSite.log	Records the activity of the Application Catalog website.	Site system server
SettingsAgent.log	Enforcement of specific applications, records orchestration of application group evaluation, and details of co-management policies.	Client
SMS_BUSINESS_APP_PROCESS_MANAGER.log	Log file for component that synchronizes apps from the Microsoft Store for Business.	Site server
SMS_CLOUDCONNECTION.log	Records information about cloud services.	Computer with the service connection point
SMSdpmon.log	Records details about the distribution point health monitoring scheduled task that is configured on a distribution point.	Site server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
SoftwareCatalogUpdateEndpoint.log	Records activities for managing the URL for the Application Catalog shown in Software Center.	Client
SoftwareCenterSystemTasks.log	Records activities related to Software Center prerequisite component validation.	Client

Packages and programs

The following table lists the log files that contain information related to deploying packages and programs.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
colleval.log	Records details about when collections are created, changed, and deleted by the Collection Evaluator.	Site server
execmgr.log	Records details about packages and task sequences that run.	Client

Asset Intelligence

The following table lists the log files that contain information related to Asset Intelligence.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
AssetAdvisor.log	Records the activities of Asset Intelligence inventory actions.	Client
aikbmgr.log	Records details about the processing of XML files from the inbox for updating the Asset Intelligence catalog.	Site server
AIUpdateSvc.log	Records the interaction of the Asset Intelligence sync point with System Center Online (SCO), the online web service.	Site system server
AIUSMSI.log	Records details about the installation of the Asset Intelligence sync point site system role.	Site system server
AIUSSetup.log	Records details about the installation of the Asset Intelligence sync point site system role.	Site system server
ManagedProvider.log	Records details about discovering software with an associated software identification tag. Also records activities related to hardware inventory.	Site system server
MVLSImport.log	Records details about the processing of imported licensing files.	Site system server

Backup and recovery

The following table lists log files that contain information related to backup and recovery actions, including site resets, and changes to the SMS Provider.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
ConfigMgrSetup.log	Records information about setup and recovery tasks when Configuration Manager recovers a site from backup.	Site server
Smsbkup.log	Records details about the site backup activity.	Site server
smssqlbkup.log	Records output from the site database backup process when SQL Server is installed on a server that isn't the site server.	Site database server
Smswriter.log	Records information about the state of the Configuration Manager VSS writer that is used by the backup process.	Site server

Certificate enrollment

The following table lists the Configuration Manager log files that contain information related to certificate enrollment. Certificate enrollment uses the certificate registration point and the Configuration Manager Policy Module on the server that's running the Network Device Enrollment Service (NDES).

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
Crp.log	Records enrollment activities.	Certificate registration point
Crpctrl.log	Records the operational health of the certificate registration point.	Certificate registration point
Crpsetup.log	Records details about the installation and configuration of the certificate registration point.	Certificate registration point
Crpmsi.log	Records details about the installation and configuration of the certificate registration point.	Certificate registration point
NDESPlugin.log	Records challenge verification and certificate enrollment activities.	Configuration Manager Policy Module and the Network Device Enrollment Service

In addition to the Configuration Manager log files, review the Windows Application logs in Event Viewer on the server running the Network Device Enrollment Service and the server hosting the certificate registration point. For example, look for messages from the **NetworkDeviceEnrollmentService** source.

You can also use the following log files:

- IIS log files for Network Device Enrollment Service: **%SYSTEMDRIVE%\inetpub\logs\LogFiles\W3SVC1**
- IIS log files for the certificate registration point: **%SYSTEMDRIVE%\inetpub\logs\LogFiles\W3SVC1**
- Network Device Enrollment Policy log file: **mscep.log**

> **NOTE**
>
> This file is located in the folder for the NDES account profile, for example, in C:\Users\SCEPSvc. For more information about how to enable NDES logging, see the Enable Logging section of the NDES wiki.

Client notification

The following table lists the log files that contain information related to client notification.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
bgbmgr.log	Records details about site server activities related to client notification tasks and processing online and task status files.	Site server
BGBServer.log	Records the activities of the notification server, such as client-server communication and pushing tasks to clients. Also records information about the generation of online and task status files to be sent to the site server.	Management point
BgbSetup.log	Records the activities of the notification server installation wrapper process during installation and uninstallation.	Management point
bgbisapiMSI.log	Records details about the notification server installation and uninstallation.	Management point
BgbHttpProxy.log	Records the activities of the notification HTTP proxy as it relays the messages of clients using HTTP to and from the notification server.	Client
CcmNotificationAgent.log	Records the activities of the notification agent, such as client-server communication and information about tasks received and dispatched to other client agents.	Client

Cloud management gateway

The following table lists the log files that contain information related to the cloud management gateway.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
CloudMgr.log	Records details about deploying the cloud management gateway service, ongoing service status, and use data associated with the service. You can configure the logging level be editing the **Logging level** value in the registry key HKLM\SOFTWARE\Microsoft\SMS\COMPONENTS\SMS_CLOUD_ SERVICES_MANAGER	The *installdir* folder on the primary site server or CAS.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
CMGSetup.log[Note 1]	Records details about the second phase of the cloud management gateway deployment (local deployment in Azure) You can configure the logging level using the setting **Trace level** (**Information** (Default), **Verbose**, **Error**) on the **Azure portal\Cloud services configuration** tab.	The **%approot%\logs** on your Azure server, or the SMS/Logs folder on the site system server
CMGHttpHandler.log[Note 1]	Records details about the cloud management gateway http handler binding with Internet Information Services in Azure You can configure the logging level using the setting **Trace level** (**Information** (Default), **Verbose**, **Error**) on the **Azure portal\Cloud services configuration** tab. Starting in version 1806, this log doesn't exist. The component functionality is merged into the CMG service component. See the CMGService.log instead.	The **%approot%\logs** on your Azure server, or the SMS/Logs folder on the site system server
CMGService.log[Note 1]	Records details about the cloud management gateway service core component in Azure You can configure the logging level using the setting **Trace level** (**Information** (Default), **Verbose**, **Error**) on the **Azure portal\Cloud services configuration** tab.	The **%approot%\logs** on your Azure server, or the SMS/Logs folder on the site system server
SMS_Cloud_ ProxyConnector.log	Records details about setting up connections between the cloud management gateway service and the cloud management gateway connection point.	Site system server
CMGContentService.log[Note 1]	Starting in version 1806, when you enable a CMG to also serve content from Azure storage, this log records the details of that service.	The **%approot%\logs** on your Azure server, or the SMS/Logs folder on the site system server

- For troubleshooting deployments, use **CloudMgr.log** and **CMGSetup.log**
- For troubleshooting service health, use **CMGService.log** and **SMS_Cloud_ProxyConnector.log**.
- For troubleshooting client traffic, use **CMGHttpHandler.log**, **CMGService.log**, and **SMS_Cloud_ProxyConnector.log**.

Note 1: Logs synchronized from Azure

These are local Configuration Manager log files that cloud service manager syncs from Azure storage every five minutes. The cloud management gateway pushes logs to Azure storage every five minutes. So the maximum delay is 10 minutes. Verbose switches affect both local and remote logs. The actual file names include the service name and role instance identifier. For example, CMG-*ServiceName*-*RoleInstanceID*-CMGSetup.log

Compliance settings and company resource access

The following table lists the log files that contain information related to compliance settings and company resource

access.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
CIAgent.log	Records details about the process of remediation and compliance for compliance settings, software updates, and application management.	Client
CITaskManager.log	Records information about configuration item task scheduling.	Client
DCMAgent.log	Records high-level information about the evaluation, conflict reporting, and remediation of configuration items and applications.	Client
DCMReporting.log	Records information about reporting policy platform results into state messages for configuration items.	Client
DcmWmiProvider.log	Records information about reading configuration item synclets from WMI.	Client

Conditional access

The following table lists the log files that contain information related to conditional access.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
ADALOperationProvider.log	Records details about acquisition of AAD token.	Client
cloudusersync.log	Records license enablement for users.	Computer with the service connection point
ComplRelayAgent.log	Receives overall compliance state from DCM, acquires MP token, acquires AAD token, and reports compliance back to Intune (the CA relay service).	Client
DcmWmiProvider.log	Records information about reading configuration item synclets from WMI.	Client
dmpdownloader.log	Records details about downloads from Microsoft Intune.	Computer with the service connection point
dmpuploader.log	Records detail related to uploading database changes to Microsoft Intune.	Computer with the service connection point
MP_Token.log	Records token requests from clients.	Site system server

Configuration Manager console

The following table lists the log files that contain information related to the Configuration Manager console.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
ConfigMgrAdminUISetup.log	Records the installation of the Configuration Manager console.	Computer that runs the Configuration Manager console
SmsAdminUI.log	Records information about the operation of the Configuration Manager console.	Computer that runs the Configuration Manager console
Smsprov.log	Records activities performed by the SMS Provider. Configuration Manager console activities use the SMS Provider.	Site server or site system server

Content management

The following table lists the log files that contain information related to content management.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
CloudDP-<guid>.log	Records details for a specific cloud-based distribution point, including information about storage and content access.	Site system server
CloudMgr.log	Records details about content provisioning, collecting storage and bandwidth statistics, and administrator-initiated actions to stop or start the cloud service that runs a cloud-based distribution point.	Site system server
DataTransferService.log	Records all BITS communication for policy or package access. This log also is used for content management by pull-distribution points.	Computer that is configured as a pull-distribution point
PullDP.log	Records details about content that the pull-distribution point transfers from source distribution points.	Computer that is configured as a pull-distribution point
PrestageContent.log	Records the details about the use of the ExtractContent.exe tool on a remote, prestaged distribution point. This tool extracts content that has been exported to a file.	Site system role
SMSdpmon.log	Records details about distribution point health monitoring scheduled tasks that are configured on a distribution point.	Site system role
smsdpprov.log	Records details about the extraction of compressed files received from a primary site. This log is generated by the WMI provider of the remote distribution point.	Distribution point computer that isn't colocated with the site server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
smsdpusage.log	Records details about the smsdpusage.exe that runs and gathers data for the distribution point usage summary report.	Site system role

Desktop Analytics

Use the following log files to help troubleshoot issues with Desktop Analytics integrated with Configuration Manager.

The log files on the service connection point are in the following directory: `%ProgramFiles%\Configuration Manager\Logs\M365A`. The log files on the Configuration Manager client are in the following directory: `%WinDir%\CCM\logs`.

LOG	DESCRIPTION	COMPUTER WITH LOG FILE
M365ADeploymentPlanWorker.log	Information about deployment plan sync from Desktop Analytics cloud service to on-premises Configuration Manager	Service connection point
M365ADeviceHealthWorker.log	Information about device health upload from Configuration Manager to Microsoft cloud	Service connection point
M365AHandler.log	Information about the Desktop Analytics settings policy	Client
M365AUploadWorker.log	Information about collection and device upload from Configuration Manager to Microsoft cloud	Service connection point
SmsAdminUI.log	Information about Configuration Manager console activity, like configuring the Azure cloud services	Service connection point

Discovery

The following table lists the log files that contain information related to discovery.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
adsgdis.log	Records Active Directory Security Group Discovery actions.	Site server
adsysdis.log	Records Active Directory System Discovery actions.	Site server
adusrdis.log	Records Active Directory User Discovery actions.	Site server
ADForestDisc.Log	Records Active Directory Forest Discovery actions.	Site server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
ddm.log	Records activities of the discovery data manager.	Site server
InventoryAgent.log	Records activities of hardware inventory, software inventory, and heartbeat discovery actions on the client.	Client
netdisc.log	Records Network Discovery actions.	Site server

Endpoint Protection

The following table lists the log files that contain information related to Endpoint Protection.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
EndpointProtectionAgent.log	Records details about the installation of the Endpoint Protection client and the application of antimalware policy to that client.	Client
EPCtrlMgr.log	Records details about the syncing of malware threat information from the Endpoint Protection role server with the Configuration Manager database.	Site system server
EPMgr.log	Monitors the status of the Endpoint Protection site system role.	Site system server
EPSetup.log	Provides information about the installation of the Endpoint Protection site system role.	Site system server

Extensions

The following table lists the log files that contain information related to extensions.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
AdminUI.ExtensionInstaller.log	Records information about the download of extensions from Microsoft, and the installation and uninstallation of all extensions.	Computer that runs the Configuration Manager console
FeatureExtensionInstaller.log	Records information about the installation and removal of individual extensions when they're enabled or disabled in the Configuration Manager console.	Computer that runs the Configuration Manager console
SmsAdminUI.log	Records Configuration Manager console activity.	Computer that runs the Configuration Manager console

Inventory

The following table lists the log files that contain information related to processing inventory data.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
dataldr.log	Records information about the processing of MIF files and hardware inventory in the Configuration Manager database.	Site server
invproc.log	Records the forwarding of MIF files from a secondary site to its parent site.	Secondary site server
sinvproc.log	Records information about the processing of software inventory data to the site database.	Site server

Metering

The following table lists the log files that contain information related to metering.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
mtrmgr.log	Monitors all software metering processes.	Client
SWMTRReportGen.log	Generates a use data report that is collected by the metering agent. This data is logged in Mtrmgr.log.	Client
swmproc.log	Records the processing of metering files and settings.	Site server

Migration

The following table lists the log files that contain information related to migration.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
migmctrl.log	Records information about migration actions that involve migration jobs, shared distribution points, and distribution point upgrades.	Top-level site in the Configuration Manager hierarchy, and each child primary site. In a multi-primary site hierarchy, use the log file created at the central administration site.

Mobile devices

The following sections list the log files that contain information related to managing mobile devices.

Enrollment

The following table lists logs that contain information related to mobile device enrollment.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
DMPRP.log	Records communication between management points that are enabled for mobile devices and the management point endpoints.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
dmpmsi.log	Records the Windows Installer data for the configuration of a management point that is enabled for mobile devices.	Site system server
DMPSetup.log	Records the configuration of the management point when it's enabled for mobile devices.	Site system server
enrollsrvMSI.log	Records the Windows Installer data for the configuration of an enrollment point.	Site system server
enrollmentweb.log	Records communication between mobile devices and the enrollment proxy point.	Site system server
enrollwebMSI.log	Records the Windows Installer data for the configuration of an enrollment proxy point.	Site system server
enrollmentservice.log	Records communication between an enrollment proxy point and an enrollment point.	Site system server
SMS_DM.log	Records communication between mobile devices, Mac computers, and the management point that is enabled for mobile devices and Mac computers.	Site system server

Exchange Server connector

The following logs contain information related to the Exchange Server connector.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
easdisc.log	Records the activities and the status of the Exchange Server connector.	Site server

Mobile device legacy

The following table lists logs that contain information related to the mobile device legacy client.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
DmCertEnroll.log	Records details about certificate enrollment data on mobile device legacy clients.	Client
DMCertResp.htm	Records the HTML response from the certificate server when the mobile device legacy client enroller program requests a PKI certificate.	Client
DmClientHealth.log	Records the GUIDs of all mobile device legacy clients that communicate with the management point that is enabled for mobile devices.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
DmClientRegistration.log	Records registration requests and responses to and from mobile device legacy clients.	Site system server
DmClientSetup.log	Records client setup data for mobile device legacy clients.	Client
DmClientXfer.log	Records client transfer data for mobile device legacy clients and for ActiveSync deployments.	Client
DmCommonInstaller.log	Records client transfer file installation for configuring mobile device legacy client transfer files.	Client
DmInstaller.log	Records whether DMInstaller correctly calls DmClientSetup, and whether DmClientSetup exits with success or failure for mobile device legacy clients.	Client
DmpDatastore.log	Records all the site database connections and queries made by the management point that is enabled for mobile devices.	Site system server
DmpDiscovery.log	Records all the discovery data from the mobile device legacy clients on the management point that is enabled for mobile devices.	Site system server
DmpHardware.log	Records hardware inventory data from mobile device legacy clients on the management point that is enabled for mobile devices.	Site system server
DmpIsapi.log	Records mobile device legacy client communication with a management point that is enabled for mobile devices.	Site system server
dmpmsi.log	Records the Windows Installer data for the configuration of a management point that is enabled for mobile devices.	Site system server
DMPSetup.log	Records the configuration of the management point when it's enabled for mobile devices.	Site system server
DmpSoftware.log	Records software distribution data from mobile device legacy clients on a management point that is enabled for mobile devices.	Site system server
DmpStatus.log	Records status messages data from mobile device clients on a management point that is enabled for mobile devices.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
DmSvc.log	Records client communication from mobile device legacy clients with a management point that is enabled for mobile devices.	Client
FspIsapi.log	Records details about communications to the fallback status point from mobile device legacy clients and client computers.	Site system server

OS deployment

The following table lists the log files that contain information related to OS deployment.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
CAS.log	Records details when distribution points are found for referenced content.	Client
ccmsetup.log	Records ccmsetup tasks for client setup, client upgrade, and client removal. Can be used to troubleshoot client installation problems.	Client
CreateTSMedia.log	Records details for task sequence media creation.	Computer that runs the Configuration Manager console
Dism.log	Records driver installation actions or update application actions for offline servicing.	Site system server
Distmgr.log	Records details about the configuration of enabling a distribution point for Preboot Execution Environment (PXE).	Site system server
DriverCatalog.log	Records details about device drivers that have been imported into the driver catalog.	Site system server
mcsisapi.log	Records information for multicast package transfer and client request responses.	Site system server
mcsexec.log	Records health check, namespace, session creation, and certificate check actions.	Site system server
mcsmgr.log	Records changes to configuration, security mode, and availability.	Site system server
mcsprv.log	Records multicast provider interaction with Windows Deployment Services (WDS).	Site system server
MCSSetup.log	Records details about multicast server role installation.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
MCSMSI.log	Records details about multicast server role installation.	Site system server
Mcsperf.log	Records details about multicast performance counter updates.	Site system server
MP_ClientIDManager.log	Records management point responses to client ID requests that task sequences initiate from PXE or boot media.	Site system server
MP_DriverManager.log	Records management point responses to Auto Apply Driver task sequence action requests.	Site system server
OfflineServicingMgr.log	Records details of offline servicing schedules and update apply actions on operating system Windows Imaging Format (WIM) files.	Site system server
Setupact.log	Records details about Windows Sysprep and setup logs. For more information, see Log Files.	Client
Setupapi.log	Records details about Windows Sysprep and setup logs.	Client
Setuperr.log	Records details about Windows Sysprep and setup logs.	Client
smpisapi.log	Records details about the client state capture and restore actions, and threshold information.	Client
Smpmgr.log	Records details about the results of state migration point health checks and configuration changes.	Site system server
smpmsi.log	Records installation and configuration details about the state migration point.	Site system server
smpperf.log	Records the state migration point performance counter updates.	Site system server
smspxe.log	Records details about the responses to clients that use PXE boot, and details about the expansion of boot images and boot files.	Site system server
smssmpsetup.log	Records installation and configuration details about the state migration point.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
SMS_PhasedDeployment.log	Log file for phased deployments	Top-level site in the Configuration Manager hierarchy
Smsts.log	Records task sequence activities.	Client
TSAgent.log	Records the outcome of task sequence dependencies before starting a task sequence.	Client
TaskSequenceProvider.log	Records details about task sequences when they're imported, exported, or edited.	Site system server
loadstate.log	Records details about the User State Migration Tool (USMT) and restoring user state data.	Client
scanstate.log	Records details about the User State Migration Tool (USMT) and capturing user state data.	Client

Power management

The following table lists the log files that contain information related to power management.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
pwrmgmt.log	Records details about power management activities on the client computer, including monitoring and the enforcement of settings by the Power Management Client Agent.	Client

Remote control

The following table lists the log files that contain information related to remote control.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
CMRcViewer.log	Records details about the activity of the remote control viewer.	On the computer that runs the remote control viewer, in the %temp% folder.

Reporting

The following table lists the Configuration Manager log files that contain information related to reporting.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
srsrp.log	Records information about the activity and status of the reporting services point.	Site system server
srsrpMSI.log	Records detailed results of the reporting services point installation process from the MSI output.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
srsrpsetup.log	Records results of the reporting services point installation process.	Site system server

Role-based administration

The following table lists the log files that contain information related to managing role-based administration.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
hman.log	Records information about site configuration changes and the publishing of site information to Active Directory Domain Services.	Site server
SMSProv.log	Records WMI provider access to the site database.	Computer with the SMS Provider

Software metering

The following table lists the log files that contain information related to software metering.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
mtrmgr.log	Monitors all software metering processes.	Site server

Software updates

The following table lists the log files that contain information related to software updates.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
AlternateHandler.log	Records details when the client calls the Office click-to-run COM interface to download and install Office 365 client updates. It's similar to use of WuaHandler when it calls the Windows Update Agent API to download and install Windows updates.	Client
ccmperf.log	Records activities related to the maintenance and capture of data related to client performance counters.	Client
DeltaDownload.log	Records information about the download of express updates and updates downloaded using Delivery Optimization.	Client

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
PatchDownloader.log	Records details about the process of downloading software updates from the update source to the download destination on the site server.	When downloading updates manually, this log file is located in the %temp% directory of the user running the console on the machine you're running the console. For Automatic Deployment Rules, this log file is located on the site server in %windir%\CCM\Logs, if the ConfigMgr client is installed on the site server.
PolicyEvaluator.log	Records details about the evaluation of policies on client computers, including policies from software updates.	Client
RebootCoordinator.log	Records details about the coordination of system restarts on client computers after software update installations.	Client
ScanAgent.log	Records details about scan requests for software updates, the WSUS location, and related actions.	Client
SdmAgent.log	Records details about the tracking of remediation and compliance. However, the software updates log file, Updateshandler.log, provides more informative details about installing the software updates that are required for compliance. This log file is shared with compliance settings.	Client
ServiceWindowManager.log	Records details about the evaluation of maintenance windows.	Client
SMS_ISVUPDATES_SYNCAGENT.log	Log file for synchronization of third-party software updates starting in Configuration Manager version 1806.	Top-level software update point in the Configuration Manager hierarchy.
SmsWusHandler.log	Records details about the scan process for the Inventory Tool for Microsoft Updates.	Client
StateMessage.log	Records details about software update state messages that are created and sent to the management point.	Client
SUPSetup.log	Records details about the software update point installation. When the software update point installation completes, **Installation was successful** is written to this log file.	Site system server

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
UpdatesDeployment.log	Records details about deployments on the client, including software update activation, evaluation, and enforcement. Verbose logging shows additional information about the interaction with the client user interface.	Client
UpdatesHandler.log	Records details about software update compliance scanning and about the download and installation of software updates on the client.	Client
UpdatesStore.log	Records details about compliance status for the software updates that were assessed during the compliance scan cycle.	Client
WCM.log	Records details about software update point configurations and connections to the WSUS server for subscribed update categories, classifications, and languages.	Site server
WSUSCtrl.log	Records details about the configuration, database connectivity, and health of the WSUS server for the site.	Site system server
wsyncmgr.log	Records details about the software update sync process.	Site server
WUAHandler.log	Records details about the Windows Update Agent on the client when it searches for software updates.	Client

Wake On LAN

The following table lists the log files that contain information related to using Wake On LAN.

> **NOTE**
> When you supplement Wake On LAN by using wake-up proxy, this activity is logged on the client. For example, see CcmExec.log and SleepAgent_<*domain*>@SYSTEM_0.log in the Client operations section of this article.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
wolcmgr.log	Records details about which clients need to be sent wake-up packets, the number of wake-up packets sent, and the number of wake-up packets retried.	Site server
wolmgr.log	Records details about wake-up procedures, such as when to wake up deployments that are configured for Wake On LAN.	Site server

Windows 10 servicing

The following table lists the log files that contain information related to Windows 10 servicing.
Servicing uses the same infrastructure and process as software updates. For other logs applicable to the servicing scenario, see Software updates.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
CBS.log	Records servicing failures related to changes for Windows Updates or roles and features.	Client
DISM.log	Records all actions using DISM. If necessary, DISM.log will point to CBS.log for more details.	Client
setupact.log	Primary log file for most errors that occur during the Windows installation process. The log file is located in the %windir%$Windows.~BT\sources\panther folder.	Client

For more information, see Online Servicing-Related Log Files.

Windows Update Agent

The following table lists the log files that contain information related to the Windows Update Agent.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
WindowsUpdate.log	Records details about when the Windows Update Agent connects to the WSUS server and retrieves the software updates for compliance assessment, and whether there are updates to the agent components.	Client

For more information, see Windows Update log files.

WSUS server

The following table lists the log files that contain information related to the WSUS server.

LOG NAME	DESCRIPTION	COMPUTER WITH LOG FILE
Change.log	Records details about WSUS server database information that has changed.	WSUS server
SoftwareDistribution.log	Records details about the software updates that are synced from the configured update source to the WSUS server database.	WSUS server

These log files are located in the `%ProgramFiles%\Update Services\LogFiles` folder.

See also

- About log files
- Support Center OneTrace
- Support Center log file viewer

- CMTrace

Release notes for Configuration Manager

9/6/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

With Configuration Manager, product release notes are limited to urgent issues. These issues aren't yet fixed in the product, or detailed in a Microsoft Support knowledge base article.

Feature-specific documentation includes information about known issues that affect core scenarios.

This article contains release notes for the current branch of Configuration Manager. For information on the technical preview branch, see Technical Preview

For information about the new features introduced with different versions, see the following articles:

- What's new in version 1906
- What's new in version 1902
- What's new in version 1810
- What's new in version 1806

TIP

To get notified when this page is updated, copy and paste the following URL into your RSS feed reader:

```
https://docs.microsoft.com/api/search/rss?search=%22release+notes+-+Configuration+Manager%22&locale=en-us
```

Set up and upgrade

Setup prerequisite warning on domain functional level on Server 2019

Applies to version 1906

When installing the update for version 1906 in an environment with domain controllers running Windows Server 2019, the prerequisite check for domain functional level returns the following warning:

```
[Completed with warning]:Verify that the Active Directory domain functional level is Windows Server 2003 or
later
```

Workaround

Ignore the warning.

Azure AD user discovery and collection group sync don't work after site expansion

Applies to version 1906

After you configure either of the following features:

- Azure Active Directory user group discovery
- Synchronize collection membership results to Azure Active Directory groups

If you then expand a standalone primary site to a hierarchy with a central administration site, you'll see the following error in SMS_AZUREAD_DISCOVERY_AGENT.log:

```
Could not obtain application secret for tenant xxxxx. If this is after a site expansion, please run "Renew
Secret Key" from admin console.
```

Workaround

Renew the key associated with the app registration in Azure AD. For more information, see Renew secret key.

Setup command-line option JoinCEIP must be specified

Applies to: Configuration Manager version 1802

Starting in Configuration Manager version 1802, the Customer Experience Improvement Program (CEIP) feature is removed from the product. When automating installation of a new site from a command-line or unattended script, setup returns an error that a required parameter is missing.

Workaround

While it has no effect on the outcome of the setup process, include the **JoinCEIP** parameter in your setup command line.

> **NOTE**
> The EnableSQM parameter for console setup is not required.

Cloud service manager component stopped on site server in passive mode

Applies to: Configuration Manager version 1806

If the service connection point is colocated with a site server in passive mode, then deployment and monitoring of a cloud management gateway doesn't start. The cloud service manager component (SMS_CLOUD_SERVICES_MANAGER) is in a stopped state.

Workaround

Move the service connection point role to another server.

OS deployment

After passive site server is promoted, the default boot image packages still have package source on the previous active server

Applies to: Configuration Manager version 1810

If you have a site server in passive mode (server B), when you promote it to active, the content location for the default boot images continues to reference the previously active server (server A). If server A has a hardware failure, you can't update or change the default boot images.

Workaround

None

Software updates

Security roles are missing for phased deployments

Applies to: Configuration Manager versions 1810, 1902

The **OS Deployment Manager** built-in security role has permissions to phased deployments. The following roles are missing these permissions:

- **Application Administrator**
- **Application Deployment Manager**
- **Software Update Manager**

The **App Author** role may appear to have some permissions to phased deployments, but shouldn't be able to create deployments.

A user with one these roles can start the Create Phased Deployment wizard, and can see phased deployments for

an application or software update. They can't complete the wizard, or make any changes to an existing deployment.

Workaround

Create a custom security role. Copy an existing security role, and add the following permissions on the **Phased Deployment** object class:

- Create
- Delete
- Modify
- Read

For more information, see Create custom security roles

Changing Office 365 client setting doesn't apply

Applies to: Configuration Manager version 1802

Deploy a client setting with **Enable Management of the Office 365 Client Agent** configured to `Yes`. Then change that setting to `No` or `Not Configured`. After updating policy on targeted clients, Office 365 updates are still managed by Configuration Manager.

Workaround

Change the following registry value to `0` and restart the **Microsoft Office Click-to-Run Service** (ClickToRunSvc):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\office\16.0\Common\officeupdate]
"OfficeMgmtCOM"=dword:00000000
```

Desktop Analytics

If you use hardware inventory for distributed views, you can't onboard to Desktop Analytics

Applies to: Configuration Manager version 1902 with update rollup, and version 1906

If you have a hierarchy, and enable **Hardware inventory** site data for distributed views on any site replication links, after you configure the Desktop Analytics connection in Configuration Manager you'll see the following error in M365UploadWorker.log:

```
Unexpected exception 'System.Data.SqlClient.SqlException' Remote access is not supported for transaction
isolation level "SNAPSHOT".: at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean
breakConnection, Action'1 wrapCloseInAction)
```

Workaround

Disable **Hardware inventory** site data for distributed views on every site replication link.

Console unexpectedly closes when removing collections

Applies to: Configuration Manager version 1902 with update rollup

After you connect the site to Desktop Analytics, you can **Select specific collections to synchronize with Desktop Analytics**. If you remove a collection and apply the changes, immediately adding a new collection causes an unhandled exception. The console unexpectedly closes.

Workaround

When you remove a collection, select **OK** to close the properties window. Then open the properties again to add a new collection on the **Desktop Analytics Connection** tab.

Pilot status tile shows some devices as 'undefined'

Applies to: Configuration Manager version 1902 with update rollup

When you use the Configuration Manager console to monitor your pilot deployment status, pilot devices that are

up-to-date on the target version of Windows for that deployment plan show as **undefined** in the Pilot status tile.

These **undefined** devices are **up-to-date** with the target version of the OS for that deployment plan. No further action is necessary.

Mobile device management

Validation for iOS app link sometimes fails on valid link

Applies to: Configuration Manager version 1810 and earlier

When you create a new application of type **App Package for iOS from App Store**, the validator doesn't accept some valid URLs for the **Location**. Specifically, the iOS App Store doesn't require a value for the app name section of the URL. For example, both of the following links are valid and point to the same app, but the **Create Application Wizard** only accepts the first:

- `https://itunes.apple.com/us/app/app-name/id123456789?mt=8`
- `https://itunes.apple.com/us/app//id123456789?mt=8`

Workaround

When you create an iOS app that's missing the app name from the URL, add any value as if it were the app name to the URL. For example:

- `https://itunes.apple.com/us/app/any-string/id123456789?mt=8`

This action allows you to complete the wizard. The app is still successfully deployed to iOS devices. The string you add to the URL appears as the **Name** on the **General Information** tab in the wizard. It's also the app's label in the Company Portal.

State messages in Configuration Manager

7/9/2019 • 10 minutes to read • Edit Online

Applies To: System Center Configuration Manager (Current Branch)

State messages contain concise information about conditions on the Configuration Manager client. The state messaging system is used by specific components of Configuration Manager, such as software updates and configuration settings.

Configuration Manager clients send state messages to fallback status point or management point site systems to report the current state of operations. You can create reports to view state messages sent by Configuration Manager clients.

Each Configuration Manager feature that uses state messages is identified by the topic type of the state message. The state message topic types listed in this article can be used to define the Configuration Manager feature that a state message relates to.

> **NOTE**
> A state message ID value of zero (0) typically indicates topic type is in an unknown state.

300 STATE_TOPICTYPE_SUM_ASSIGNMENT_COMPLIANCE

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
0	Compliance state unknown
1	Compliant
2	Non-compliant

301 STATE_TOPICTYPE_SUM_ASSIGNMENT_ENFORCEMENT

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
0	Enforcement state unknown
1	Installing update(s)
2	Waiting for restart
3	Waiting for another installation to complete
4	Successfully installed update(2)
5	Pending system restart
6	Failed to install the update(s)

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
7	Downloading the update(s)
8	Downloaded update(s)
9	Failed to download update(s)
10	Waiting for the maintenance window before installing
11	Waiting for orchestration

302 STATE_TOPICTYPE_SUM_ASSIGNMENT_EVALUATION

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
0	Evaluation state unknown
1	Evaluation activated
2	Evaluation succeeded
3	Evaluation failed

400 STATE_TOPICTYPE_SUM_CI_DETECTION

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
0	Detection state unknown
1	Not required
2	Not detected
3	Detected

401 STATE_TOPICTYPE_SUM_CI_COMPLIANCE

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
0	Compliance state unknown
1	Compliant
2	Non-compliant
3	Conflict detected
4	Error

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
5	Unknown
6	Partial compliance
7	Compliance not configured

402 STATE_TOPICTYPE_SUM_CI_ENFORCEMENT

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
0	Enforcement state unknown
1	Enforcement started
2	Enforcement waiting for content
3	Waiting for another installation to complete
4	Waiting for the maintenance window before installing
5	Restart required before installing
6	General failure
7	Pending installation
8	Installing update
9	Pending system restart
10	Successfully installed update
11	Failed to install the update
12	Downloading update
13	Downloaded update
14	Failed to download the update

500 STATE_TOPTCTYPE_SUM_UPDATE_DETECTION

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
0	Detection state unknown
1	Update is not required
2	Update is required

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
3	Update is installed

501 STATE_TOPICTYPE_SUM_UPDATE_SOURCE_SCAN

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
0	Scan state unknown
1	Scan is waiting for content
2	Scan is running
3	Scan complete
4	Scan is pending retry
5	Scan failed
6	Scan completed with errors

700 STATE_TOPICTYPE_RESYNC_STATE_MSG

No State IDs.

701 STATE_TOPICTYPE_SYSTEM_HEARTBEAT

No State IDs.

702 STATE_TOPICTYPE_CKD_UPDATE

No State IDs.

800 STATE_TOPICTYPE_CLIENT_DEPLOYMENT

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
100	Client deployment started
101	Waiting for download
102	Deployment Scheduled
103	Waiting for the window before deploying
104	Deployment skipped
301	Unknown client deployment failure
302	Failed to create the ccmsetup service

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
303	Failed to delete the ccmsetup service
304	Cannot install over embedded operating system with File-Based Write Filter (FBWF) enabled on the system drive
305	Native security mode is not valid on Windows 2000
306	Failed to start ccmsetup download process
307	Non-valid ccmsetup command line
308	Failed to download the file over WINHTTP at address
309	Failed to download the files through BITS at address
310	Failed to install BITS version
311	Can't verify that prerequisite file is MS signed
312	Failed to copy the file because the disk is full
313	Client.msi installation failed with MSI error
314	Failed to load ccmsetup.xml manifest file
315	Failed to obtain a client certificate
316	Prerequisite file is not MS signed
317	Reboot required to continue the installation
318	Cannot install the client on the MP because the MP and client versions do not match
319	Operating system or service pack not supported
320	Deployment not supported
321	Bits Missing
322	Source folder is unavailable
323	Appv not supported
324	Incorrect Site Version
325	Prerequisite hash mismatch
326	MDM Deregistration Failed

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
327	MDM Registration Detected
328	Intune Detected
329	Metered Network Disallowed
400	Client deployment succeeded
401	Deployment Succeeded Reboot Required
402	Deployment Succeeded Reboot Succeeded
500	Client assignment started
601	Unknown client assignment failure
602	The following site code is invalid
603	Failed to assign to MP
604	Failed to discover default management point
605	Failed to download site signing certificate
606	Failed to auto discover site code
607	Site assignment failed; client version higher than site version
608	Failed to get Site Version from Active Directory Domain Services and SLP
609	Failed to get client version
700	Client assignment succeeded

801 STATE_TOPICTYPE_DEVICE_CLIENT_DEPLOYMENT

No State IDs.

810 STATE_TOPICTYPE_CLIENT_COMANAGEMENT

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
100	Enrollment status
101	Enrollment scheduled
102	Enrollment canceled
105	Enrollment started

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
106	Enrollment succeeded but is not provisioned
107	Enrollment succeeded and is provisioned
108	Enrollment no active user
110	Enrollment failed

820 STATE_TOPICTYPE_CLIENT_WUFB

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Windows Update for Business client status

900 STATE_TOPICTYPE_BRANCH_DP

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Disk Space

901 STATE_TOPICTYPE_REMOTE_DP_MONITORING

No State IDs.

902 STATE_TOPICTYPE_PULL_DP_MONITORING

No State IDs.

903 STATE_TOPICTYPE_DP_USAGE

No State IDs.

1000 STATE_TOPICTYPE_CLIENT_FRAMEWORK_COMM

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Client is successfully communicating with the management point
2	Client failed to communicate with the management point

1001 STATE_TOPICTYPE_CLIENT_FRAMEWORK_LOCAL

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Client successfully retrieved the certificate from the local certificate store

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
2	Client failed to retrieve the certificate from the local certificate store

1002 STATE_TOPICTYPE_DEVICE_CLIENT_FRAMEWORK_COMM

No State IDs.

1003 STATE_TOPICTYPE_DEVICE_CLIENT_FRAMEWORK_LOCAL

No State IDs.

1004 STATE_TOPICTYPE_DEVICE_CLIENT_FRAMEWORK_CERTIFICATE

No State IDs.

1005 STATE_TOPICTYPE_DEVICE_CLIENT_WIPE

No State IDs.

1006 STATE_TOPICTYPE_DEVICE_CLIENT_RETIRE

No State IDs.

1007 STATE_TOPICTYPE_DEVICE_CLIENT_WIPE_INTUNE

No State IDs.

1008 STATE_TOPICTYPE_DEVICE_CLIENT_RETIRE_INTUNE

No State IDs.

1009 STATE_TOPICTYPE_DEVICE_CLIENT_DEVICELOCK

No State IDs.

1010 STATE_TOPICTYPE_DEVICE_CLIENT_DEVICELOCK_INTUNE

No State IDs.

1011 STATE_TOPICTYPE_DEVICE_CLIENT_DEVICEPINRESET

No State IDs.

1012 STATE_TOPICTYPE_DEVICE_CLIENT_DEVICEPINRESET_INTUNE

No State IDs.

1013 STATE_TOPICTYPE_DEVICE_CLIENT_DEVICEPINRESET_ONPREM

No State IDs.

1014 STATE_TOPICTYPE_DEVICE_CLIENT_DEVICEALBYPASS

No State IDs.

1015 STATE_TOPICTYPE_DEVICE_CLIENT_DEVICEALBYPASS_INTUNE

No State IDs.

1100 STATE_TOPICTYPE_CLIENT_FRAMEWORK_MODEREADINESS

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Client not ready for native mode
2	Client ready for native mode

1300 STATE_TOPICTYPE_CLIENT_HEALTH

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Success
2	Not successful

1401 STATE_TOPICTYPE_STATE_REPORT

No State IDs.

1500 STATE_TOPICTYPE_CAL_TRACK_UT

No State IDs.

1502 STATE_TOPICTYPE_CAL_TRACK_MT

No State IDs.

1503 STATE_TOPICTYPE_CAL_TRACK_ML

No State IDs.

1600 STATE_TOPICTYPE_USER_AFFINITY

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	User affinity set
2	User affinity removed

1700 STATE_TOPICTYPE_APP_CI_SCAN

No State IDs.

1701 STATE_TOPICTYPE_APP_CI_COMPLIANCE

No State IDs.

1702 STATE_TOPICTYPE_APP_CI_ENFORCEMENT

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1000	Configuration Item succeeded
1001	Configuration Item succeeded already installed
1002	Configuration Item succeeded preflight
1003	Configuration Item fast status succeeded
2000	Configuration Item in progress
2001	Configuration Item in progress waiting for content
2002	Configuration Item in progress installing
2003	Configuration Item in progress waiting reboot
2004	Configuration Item in progress waiting for maintenance window
2005	Configuration Item in progress waiting schedule
2006	Configuration Item in progress downloading dependent content
2007	Configuration Item in progress installing dependencies
2008	Configuration Item in progress pending reboot
2009	Configuration Item in progress content downloaded
2010	Configuration Item in progress pending update
2011	Configuration Item in progress waiting user reconnect
2012	Configuration Item in progress waiting for user sign out
2013	Configuration Item in progress waiting for user sign in
2014	Configuration Item in progress waiting for install
2015	Configuration Item in progress waiting for retry
2016	Configuration Item in progress waiting for presmode

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
2017	Configuration Item in progress waiting for orchestration
2018	Configuration Item in progress waiting for network
2019	Configuration Item in progress pending update VE
2020	Configuration Item in progress updating VE
3000	Configuration Item requirements not met
3001	Configuration Item requirements not met host not applicable
4000	Configuration Item unknown
5000	Configuration Item error
5001	Configuration Item error evaluating
5002	Configuration Item error installing
5003	Configuration Item error retrieving content
5004	Configuration Item error installing dependency
5005	Configuration Item error retrieving content dependency
5006	Configuration Item error rules conflict
5007	Configuration Item error waiting for retry
5008	Configuration Item error uninstalling supersedence
5009	Configuration Item error downloading superseded
5010	Configuration Item error updating VE
5011	Configuration Item error installing license
5012	Configuration Item error retrieving allow all trusted apps
5013	Configuration Item error no licenses available
5014	Configuration Item error OS not supported
6000	Configuration Item launch succeeded
6010	Configuration Item launch error
6020	Configuration Item launch unknown

1703 STATE_TOPICTYPE_APP_CI_ASSIGNMENT_EVALUATIO

No State IDs.

1704 STATE_TOPICTYPE_APP_CI_LAUNCH

No State IDs.

1800 STATE_TOPICTYPE_EVENT_INTRINSIC

No State IDs.

1801 STATE_TOPICTYPE_EVENT_EXTRINSIC

No State IDs.

1900 STATE_TOPICTYPE_EP_AM_INFECTION

No State IDs.

1901 State_Topictype_Ep_Am_Health

No State IDs.

1902 STATE_TOPICTYPE_EP_MALWARE

No State IDs.

1950 STATE_TOPICTYPE_ATP_HEALTH_STATUS

No State IDs.

2001 STATE_TOPICTYPE_EP_CLIENT_DEPLOYMENT

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Endpoint Protection unmanaged
2	Endpoint Protection waiting for install
3	Endpoint Protection managed
4	Endpoint Protection installation failed
5	Endpoint Protection reboot pending
6	Endpoint Protection not supported
7	Endpoint Protection co-managed

2002 STATE_TOPICTYPE_EP_CLIENT_POLICYAPPLICATION

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
0	Endpoint Protection policy application status unknown
1	Endpoint Protection policy application succeeded
2	Endpoint Protection policy application failed

2003 STATE_TOPICTYPE_CLIENT_ACTION

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
0	Unknown
1	Active
2	Inactive

2100 STATE_TOPICTYPE_WP_CLIENT_DEPLOYMENT

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Wakeup Proxy is not installed
2	Wakeup Proxy is waiting for installation
3	Wakeup Proxy is installed
4	Wakeup Proxy installation failed
5	Wakeup Proxy is waiting for reboot
6	Wakeup Proxy is not supported on this OS
7	Wakeup Proxy server opt out
8	Wakeup Proxy uninstall failed
9	Wakeup Proxy runtime not supported

2200 STATE_TOPICTYPE_FDM

No State IDs.

2201 STATE_TOPICTYPE_CCM_CERT_BINDING

No State IDs.

2202 STATE_TOPICTYPE_SERVER_STATISTIC

No State IDs.

3000 STATE_TOPICTYPE_DM_WNS_CHANNEL

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
0	Windows Push Notification service channel set

4000 STATE_TOPICTYPE_MDM_DEVICE_PROPERTY

No State IDs.

4002 STATE_TOPICTYPE_MDM_CLIENT_IDENITITY

No State IDs.

4003 STATE_TOPICTYPE_MDM_APPLICATION_REQUEST

No State IDs.

4004 STATE_TOPICTYPE_MDM_APPLICATION_STATE

No State IDs.

4005 STATE_TOPICTYPE_MDM_LICENSE_DEVICE_RELATION

No State IDs.

4006 STATE_TOPICTYPE_MDM_LICENSE_KEYS

No State IDs.

4007 STATE_TOPICTYPE_MDM_POLICY_ASSIGNMENT

No State IDs.

4008 STATE_TOPICTYPE_MDM_ANDROID_COUNT

No State IDs.

4009 STATE_TOPICTYPE_MDM_SLK_STATUS

No State IDs.

4010 STATE_TOPICTYPE_MDM_USER_COMPANY_TERM_ACCEPTANCE

No State IDs.

4022 STATE_TOPICTYPE_MDM_DEP_SYNCNOW_STATUS

No State IDs.

4023 STATE_TOPICTYPE_MDM_MAM_STORE_APP_SYNC

No State IDs.

5000 STATE_TOPICTYPE_CERTIFICATE_ENROLLMENT

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Challenge issued
2	Challenge issue failed
3	Request creation failed
4	Request submit failed
5	Challenge validation succeeded
6	Challenge validation failed
7	Issue failed
8	Issue pending
9	Issued
10	Response processing failed
11	Response pending
12	Enrollment succeeded
13	Enrollment not needed
14	Revoked
15	Removed from collection
16	Renew verified
17	Install failed
18	Installed
19	Delete failed
20	Deleted
21	Renewal requested

5001 STATE_TOPICTYPE_CERTIFICATE_CRP

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Challenge issued
2	Challenge issue failed
3	Request creation failed
4	Request submit failed
5	Challenge validation succeeded
6	Challenge validation failed
7	Issue failed
8	Issue pending
9	Issued
10	Response processing failed
11	Response pending
12	Enrollment succeeded
13	Enrollment not needed
14	Revoked
15	Removed from collection
16	Renew verified
17	Install failed
18	Installed
19	Delete failed
20	Deleted
21	Renewal requested

5200 STATE_TOPICTYPE_RESOURCE_ACCESS_STATUS

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Status pin setup succeeded
2	Status pin setup failed

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
3	Status pin setup not supported
4	Status pin setup in progress

6000 STATE_TOPICTYPE_REMOTEAPP_SUBSCRIPTION_STATUS

No State IDs.

6001 STATE_TOPICTYPE_REMOTEAPP_SUBSCRIPTION_SYNC_STATUS

No State IDs.

6002 STATE_TOPICTYPE_REMOTEAPP_AUTHCOOKIES_SYNC_STATUS

No State IDs.

6003 STATE_TOPICTYPE_REMOTEAPPLICATIONS_SYNC_STATUS

No State IDs.

6004 STATE_TOPICTYPE_REMOTEAPP_LOCK_RESULT

No State IDs.

7000 STATE_TOPICTYPE_USER_COMPANY_TERM_ACCEPTANCE

No State IDs.

7001 STATE_TOPICTYPE_PFX_CERTIFICATE

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Challenge issued
2	Challenge issue failed
3	Request creation failed
4	Request submit failed
5	Challenge validation succeeded
6	Challenge validation failed
7	Issue failed
8	Issue pending
9	Issued

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
10	Response processing failed
11	Response pending
12	Enrollment succeeded
13	Enrollment not needed
14	Revoked
15	Removed from collection
16	Renew verified
17	Install failed
18	Installed
19	Delete failed
20	Deleted
21	Renewal requested

7010 STATE_TOPICTYPE_CONDITIONAL_ACCESS_COMPLIANCE

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION	
	1	Compliance success
2	Compliance fail at mp	
3	Compliance fail at the client	
4	Compliance fail at Intune	
5	Compliance fail at AAD	
6	Compliance comgmt Intune	

7200 STATE_TOPICTYPE_SUPER_PEER_UPDATE_CACHE_MAP

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Peer Cache Source added
2	Peer Cache Source removed

7201 STATE_TOPICTYPE_SUPER_PEER_UPDATE_CONFIG

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Peer Cache Source deactivated
2	Peer Cache Source is active

7202 STATE_TOPICTYPE_DOWNLOAD_AGGREGATE_DATA

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Download aggregate data upload

7203 STATE_TOPICTYPE_PEERSOURCE_REQ_REJECTION_STATS

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Peer source rejection data upload

7300 STATE_TOPICTYPE_PROXY_TRAFFIC

No State IDs.

7301 STATE_TOPICTYPE_PROXY_CONNECTION

No State IDs.

7302 STATE_TOPICTYPE_SRS_USAGE_DATA

No State IDs.

7303 STATE_TOPICTYPE_PROXY_TRAFFIC_IDENTITY

No State IDs.

8001 STATE_TOPICTYPE_HAS_REPORT

STATE MESSAGE ID	STATE MESSAGE DESCRIPTION
1	Health attestation is supported
2	Health attestation is not supported

STATE_TOPICTYPE_DEVICE_CLIENT_EDPLOG

No State IDs.

8003 STATE_TOPICTYPE_ENABLE_LOSTMODE

No State IDs.

8004 STATE_TOPICTYPE_DISABLE_LOSTMODE

No State IDs.

8005 STATE_TOPICTYPE_LOCATE_DEVICE

No State IDs.

8006 STATE_TOPICTYPE_REBOOT_DEVICE

No State IDs.

8007 STATE_TOPICTYPE_LOGOUTUSER

No State IDs.

8008 STATE_TOPICTYPE_USERSLIST

No State IDs.

8009 STATE_TOPICTYPE_DELETEUSER

No State IDs.

8010 STATE_TOPICTYPE_CLEANPCRETAININGUSERDATA

No State IDs.

8011 STATE_TOPICTYPE_CLEANPCWITHOUTRETAININGUSERDATA

No State IDs.

8012 STATE_TOPICTYPE_SETDEVICENAME

No State IDs.

9000 STATE_TOPICTYPE_BOOK_CI_COMPLIANCE

No State IDs.

9001 STATE_TOPICTYPE_BOOK_CI_ENFORCEMENT

No State IDs.

Next steps

- Description of state messaging in Configuration Manager
- Software updates management whitepaper for Configuration Manager

Unicode and ASCII support in Configuration Manager

8/30/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager creates most objects by using Unicode characters. However, several objects only support ASCII characters, or they have other limitations.

Objects that use ASCII characters

When you create the following objects, Configuration Manager only supports the ASCII character set:

- Site code
- All site system server computer names
- The following Configuration Manager accounts:

  > **NOTE**
  > These accounts support ASCII characters, and RUS characters on a site that runs in Russian.

  - Client push installation account
  - Management point database connect account
  - Network access account
  - Package access account
  - Standard sender account
  - Site system installation account
  - Software update point connection account
  - Software update point proxy server account

  > **NOTE**
  > The accounts that you specify for role-based administration support Unicode.
  >
  > The reporting services point account supports Unicode, with the exception of RUS characters.

- Fully qualified domain name (FQDN) for site servers and site systems
- Installation path for Configuration Manager
- SQL Server instance names
- The path for the following site system roles:
  - Enrollment point

    - Enrollment proxy point
    - Reporting services point
    - State migration point
- The path for the following folders:
    - The folder that stores client state migration data
    - The folder that contains the Configuration Manager reports
    - The folder that stores the Configuration Manager backup
    - The folder that stores the installation source files for site setup
    - The folder that stores the prerequisite downloads for use by setup
- The path for the following objects:
    - IIS website
    - Virtual application installation path
    - Virtual application name
- Boot media ISO file names

Additional limitations

The following are additional limitations for supported character sets and language versions:

- Configuration Manager doesn't support changing the locale of the site server computer.
- An enterprise certificate authority (CA) doesn't support client computer names that use double-byte character sets (DBCS). The client computer names that you can use are restricted by the PKI limitation of the IA5 character set. Configuration Manager doesn't support CA names or subject name values that use DBCS.

Objects that aren't localized

The Configuration Manager database supports Unicode for most objects that it stores. When possible, it displays this information in the OS language that matches the locale of a computer. For the client interface or Configuration Manager console to display information in the computer's OS language, the computer's locale must match a client or server language that you install at a site.

Several Configuration Manager objects don't support Unicode. They're stored in the database by using ASCII, or they have additional language limitations. This information is always displayed by using the ASCII character set, or in the language that was in use when you created the object.

Management insights in Configuration Manager

8/9/2019 • 9 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Management insights in Configuration Manager provide information about the current state of your environment. The information is based on analysis of data from the site database. Insights help you to better understand your environment and take action based on the insight. This feature was released in Configuration Manager version 1802.

Review management insights

To view the rules, your account needs the **read** permission on the **site** object.

1. Open the Configuration Manager Console.
2. Go to the **Administration** workspace, expand **Management Insights**, and select **All Insights**.

   > **NOTE**
   > Starting in version 1810, when you select the **Management Insights** node, it shows the Management insights dashboard.

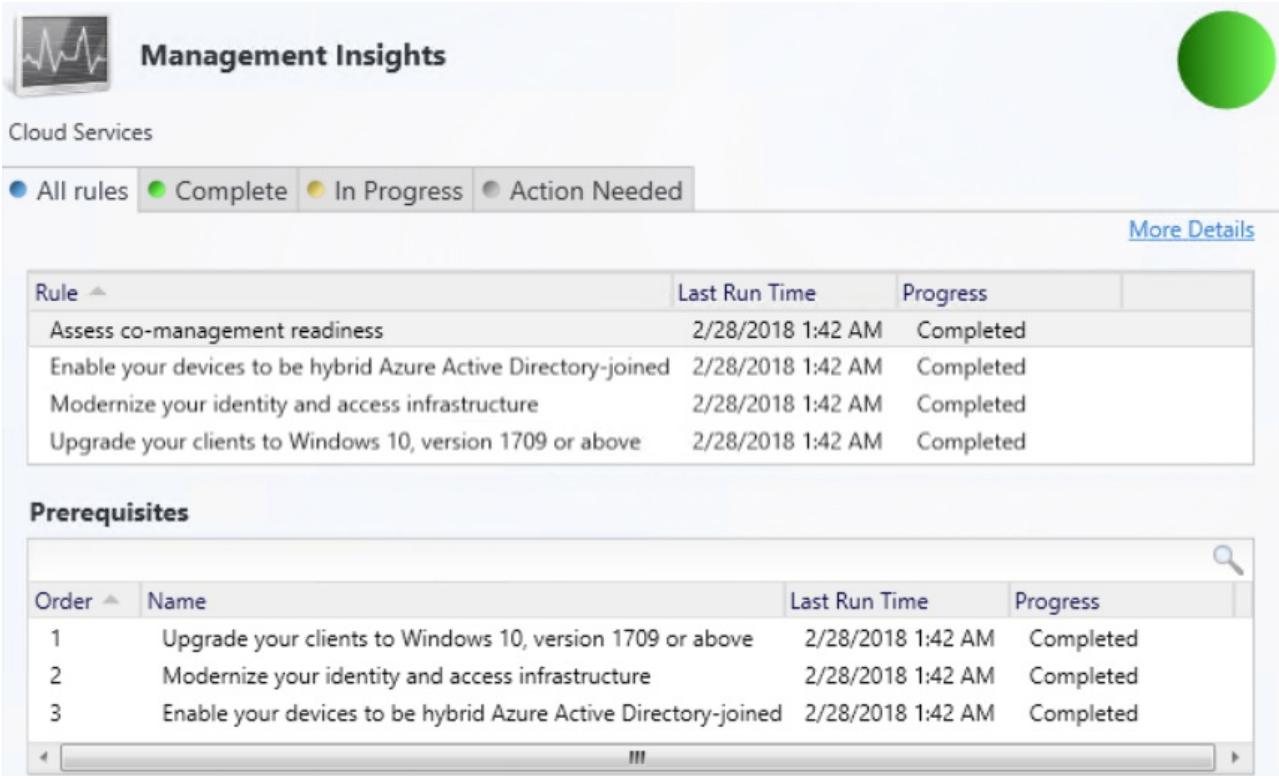
3. Open the management insights group name you want to review. Select **Show Insights** in the ribbon.

The following four tabs are available for review:

- **All Rules**: Gives the complete list of rules for the management insight group chosen.
- **Complete**: Lists rules where no action is needed.
- **In Progress**: Shows rules where some, but not all, prerequisites are complete.
- **Action Needed**: Rules needing actions taken are listed. Select **More Details** to retrieve specific items where action is needed.

The **Prerequisites** pane lists the required items needed to run the rule.

All rules and prerequisites for the cloud services group



Select a rule and then select **More Details** to see the rule details.

Operations

The management insight rules reevaluate their applicability on a weekly schedule. To reevaluate a rule on-demand, right-click the rule and select **Re-evaluate**.

The log file for management insight rules is **SMS_DataEngine.log** on the site server.

Starting in version 1806, some rules let you take action. Select a rule, select **More Details**, and then if available select **Take action**.

Depending upon the rule, this action has one of the following behaviors:

- Automatically navigate in the console to the node where you can take further action. For example, if the management insight recommends changing a client setting, taking action navigates to the Client Settings node. Then take further action by modifying the default or a custom client settings object.
- Navigate to a filtered view based on a query. For example, taking action on the empty collections rule shows just these collections in the list of collections. Then take further action, such as deleting a collection or modifying its membership rules.

Management insights dashboard

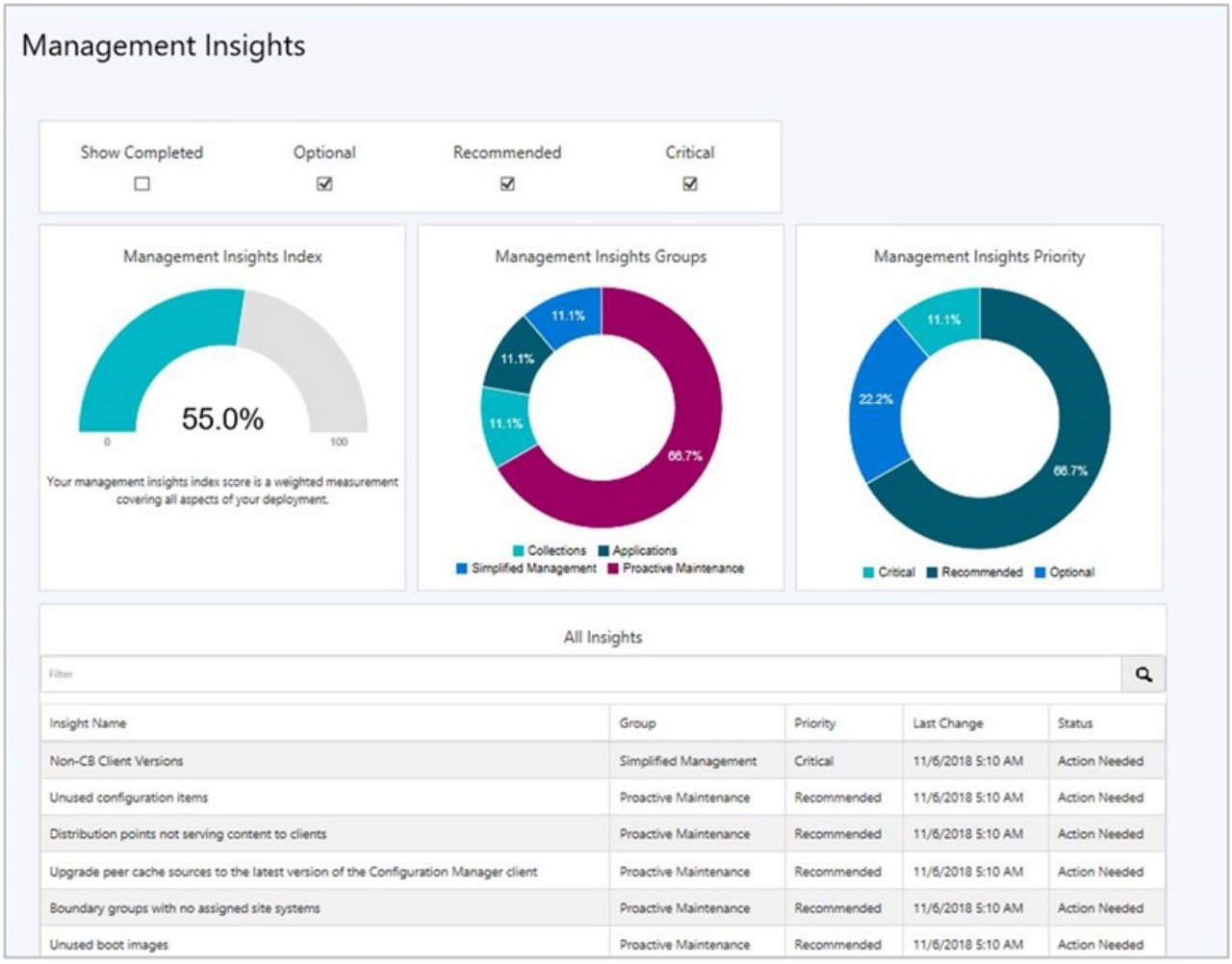
Starting in version 1810, the **Management Insights** node includes a graphical dashboard. This dashboard displays an overview of the rule states, which makes it easier for you to show your progress.

Use the following filters at the top of the dashboard to refine the view:

- Show Completed
- Optional
- Recommended
- Critical

The dashboard includes the following tiles:

- **Management insights index**: Tracks overall progress on management insights rules. The index is a weighted average. Critical rules are worth the most. This index gives the least weight to optional rules.
- **Management insights groups**: Shows percent of rules in each group, honoring the filters. Select a group to drill down to the specific rules in this group.
- **Management insights priority**: Shows percent of rules by priority, honoring the filters.
- **All insights**: A table of insights including priority and state. Use the **Filter** field at the top of the table to match strings in any of the available columns. The dashboard sorts the table in the following order:
  - Status: Action Needed, Completed, Unknown
  - Priority: Critical, Recommended, Optional
  - Last Changed: older dates on top



Groups and rules

Rules are organized into the following management insight groups:

- Applications
- Cloud services
- Collections
- Proactive maintenance
- Security
- Simplified management
- Software Center
- Windows 10

Applications

Insights for your application management.

- **Applications without deployments**: Lists the applications in your environment that don't have active deployments. This rule helps you find and delete unused applications to simplify the list of applications displayed in the console. For more information, see Deploy applications.

Cloud services

Helps you integrate with many cloud services, which enable modern management of your devices.

- **Assess co-management readiness**: Helps you understand what steps are needed to enable co-management. This rule has prerequisites. For more information, see Co-management overview.
- **Configure Azure services for use with Configuration Manager**: This rule helps you onboard Configuration Manager to Azure AD, which enables clients to authenticate with the site using Azure AD. For more information, see Configure Azure services.
- **Enable devices to be hybrid Azure Active Directory joined**: Azure AD-joined devices allow users to sign in with their domain credentials while ensuring devices meet the organization's security and compliance standards. For more information, see Azure AD hybrid identity design considerations.
- **Update clients to the latest Windows 10 version**: Windows 10, version 1709 or above improves and modernizes the computing experience of your users. For more information, see Key articles about adopting Windows as a service.

Collections

Insights that help simplify management by cleaning up and reconfiguring collections.

- **Empty Collections**: Lists collections in your environment that have no members. For more information, see How to manage collections.

Starting in version 1902, there are new rules with recommendations on managing collections. Use these insights to simplify management and improve performance:

- **Collections with no query rules and no direct members**: To simplify the list of collections in your hierarchy, delete these collections.
- **Collections with the same re-evaluation start time**: These collections have the same re-evaluation time as other collections. Modify the re-evaluation time so they don't conflict.
- **Collections with query time over two seconds**: Review the query rules for this collection. Consider modifying or deleting the collection.
- The following rules include configurations that potentially cause unnecessary load on the site. Review these collections, then either delete them, or disable rule evaluation:
  - **Collections with no query rules and incremental updates enabled**
  - **Collections with no query rules and enabled for scheduled or incremental evaluation**
  - **Collections with no query rules and schedule full evaluation selected**

Proactive maintenance

Starting in version 1806, the rules in this group highlight potential configuration issues to avoid through upkeep of Configuration Manager objects.

- **Boundary groups with no assigned site systems**: Without assigned site systems, boundary groups can only be used for site assignment. For more information, see Configure boundary groups.

- **Boundary groups with no members**: Boundary groups aren't applicable for site assignment or content lookup if they don't have any members. For more information, see Configure boundary groups.
- **Distribution points not serving content to clients**: Distribution points that haven't served content to clients in the past 30 days. This data is based on reports from clients of their download history. For more information, see Install and configure distribution points.
- **Enable WSUS Cleanup**: Verifies that you've enabled the option to run WSUS cleanup on the properties of the software update point component. This option helps to improve WSUS performance. For more information, see Software update maintenance.
- **Unused boot images**: Boot images not referenced for PXE boot or task sequence use. For more information, see Manage boot images.
- **Unused configuration items**: Configuration items that aren't part of a configuration baseline and are older than 30 days. For more information, see Create configuration baselines.
- **Upgrade peer cache sources to the latest version of the Configuration Manager client**: Identify clients that serve as a peer cache source but haven't upgraded from a pre-1806 client version. Pre-1806 clients can't be used as a peer cache source for clients that run version 1806 or later. Select **Take action** to open a device view that displays the list of clients.

Security

Insights for improving the security of your infrastructure and devices.

- **NTLM fallback is enabled**: Starting in version 1906, this rule detects if you enabled the less secure NTLM authentication fallback method for the site. When using the client push method of installing the Configuration Manager client, the site can require Kerberos mutual authentication. This enhancement helps to secure the communication between the server and the client. For more information, see How to install clients with client push.
- **Unsupported antimalware client versions**: More than 10% of clients are running versions of System Center Endpoint Protection that aren't supported. For more information, see Endpoint Protection.

Simplified management

Insights that help you simplify the day-to-day management of your environment.

- **Connect the site to the Microsoft cloud for Configuration Manager updates**: This rule makes sure your Configuration Manager service connection point has connected to the Microsoft cloud within the past seven days. This connection is to download content for regular updates. Review DMPDownloader.log and hman.log. For more information, see Internet access requirements.
- **Non-CB Client Versions**: Lists all clients whose versions aren't a current branch (CB) build. For more information, see Upgrade clients.
- **Update clients to a supported Windows 10 version**: Starting in version 1902, this rule reports on clients that are running a version of Windows 10 that's no longer supported. It also includes clients with a Windows 10 version that's near end of service (three months).

Software Center

Insights for managing Software Center.

- **Direct users to Software Center instead of Application Catalog**: Check if users have installed or requested applications from the application catalog in the last 14 days. The primary functionality of application catalog is now included in Software Center. The application catalog is deprecated. For more information, see Deprecated features.
- **Use the new version of Software Center**: The previous version of Software Center is no longer

supported. Set up clients to use the new Software Center by enabling the client setting **Use new Software Center** in the **Computer Agent** group. For more information, see About client settings.

Software Updates

- **Client settings aren't configured to allow clients to download delta content**: Some software updates synchronized in your environment include delta content. Enable the client setting, **Allow clients to download delta content when available**. If you don't enable this setting, when you deploy these updates, client will unnecessarily download more content than they require. For more information, see Client settings - Software updates.

- **Enable the software updates product category 'Windows 10, version 1903 and later'**: There's a new software updates product category for Windows 10, version 1903 and later. If you synchronize Windows 10 updates and have Windows 10, version 1903 or later clients, select the **Windows 10, version 1903 and later** product category in the software update point component properties. For more information, seeConfigure classifications and products to synchronize.

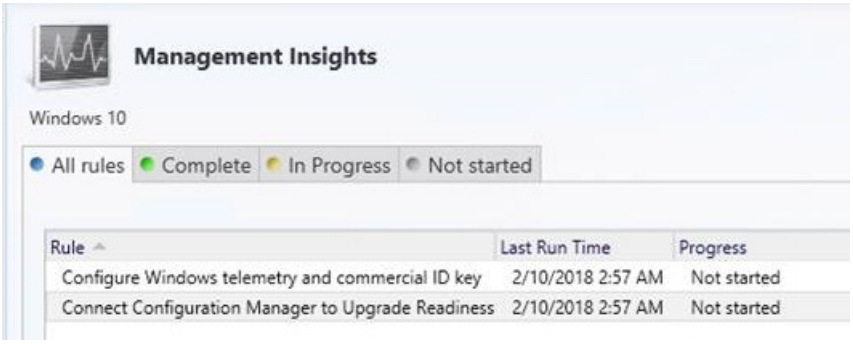
Windows 10

Insights related to the deployment and servicing of Windows 10. The Windows 10 management insight group is only available when more than half of clients are running Windows 7, Windows 8, or Windows 8.1.

- **Configure Windows telemetry and commercial ID key**: To use data from Upgrade Readiness, configure devices with a Commercial ID key and enable collection of diagnostic data. Set Windows 10 devices to **Enhanced (Limited)** level or higher. For more information, see Configure clients to report data to Windows Analytics.

- **Connect Configuration Manager to Upgrade Readiness**: Use Upgrade Readiness for your Windows 10 deployments before Windows 7 goes out of support. For more information, see Integrate Upgrade Readiness.

Windows 10 management insights rules



CMPivot for real-time data in Configuration Manager

9/11/2019 • 22 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager has always provided a large centralized store of device data, which customers use for reporting purposes. The site typically collects this data on a weekly basis. Starting in version 1806, CMPivot is a new in-console utility that now provides access to real-time state of devices in your environment. It immediately runs a query on all currently connected devices in the target collection and returns the results. Then filter and group this data in the tool. By providing real-time data from online clients, you can more quickly answer business questions, troubleshoot issues, and respond to security incidents.

For example, in mitigating speculative execution side channel vulnerabilities, one of the requirements is to update the system BIOS. You can use CMPivot to quickly query on system BIOS information, and find clients that aren't in compliance.

> **TIP**
> Some security software may block scripts running from c:\windows\ccm\scriptstore. This can prevent successful execution of CMPivot queries. Some security software may also generate audit events or alerts when running CMPivot PowerShell.

Prerequisites

The following components are required to use CMPivot:

- Upgrade the target devices to the latest version of the Configuration Manager client.
- Target clients require a minimum of PowerShell version 4.
- To gather data for the following entities, target clients require PowerShell version 5.0:
  - Administrators
  - Connection
  - IPConfig
  - SMBConfig
- Permissions for CMPivot:
  - **Read** permission on the **SMS Scripts** object
  - **Run Scripts** permission on the **Collection**
    - Alternatively, starting in version 1906, you can use **Run CMPivot** on **Collection**.
  - **Read** permission on **Inventory Reports**
  - The default scope.

> **NOTE**
> **Run Scripts** is a super set of the **Run CMPivot** permission.

Limitations

- In a hierarchy, connect the Configuration Manager console to a *primary site* to run CMPivot. The **Start**

CMPivot action doesn't appear in the console when it's connected to a central administration site (CAS).

  - Starting in Configuration Manager version 1902, you can run CMPivot from a CAS. In some environments, additional permissions are needed. For more information, see CMPivot starting in version 1902.

- CMPivot only returns data for clients connected to the current site.
- If a collection contains devices from another site, CMPivot results are only from devices in the current site.
- You can't customize entity properties, columns for results, or actions on devices.
- Only one instance of CMPivot can run at the same time on a computer that is running the Configuration Manager console.
- In version 1806, the query for the **Administrators** entity only works if the group is named "Administrators". It doesn't work if the group name is localized. For example, "Administrateurs" in French.

Start CMPivot

1. In the Configuration Manager console, connect to the primary site. Go to the **Assets and Compliance** workspace, and select the **Device Collections** node. Select a target collection, and click **Start CMPivot** in the ribbon to launch the tool.

   > **TIP**
   > If you don't see this option, check the following configurations:
   >
   > - Confirm with a site administrator that your account has the required permissions. For more information, see Prerequisites.
   > - Connect the console to a *primary site*.

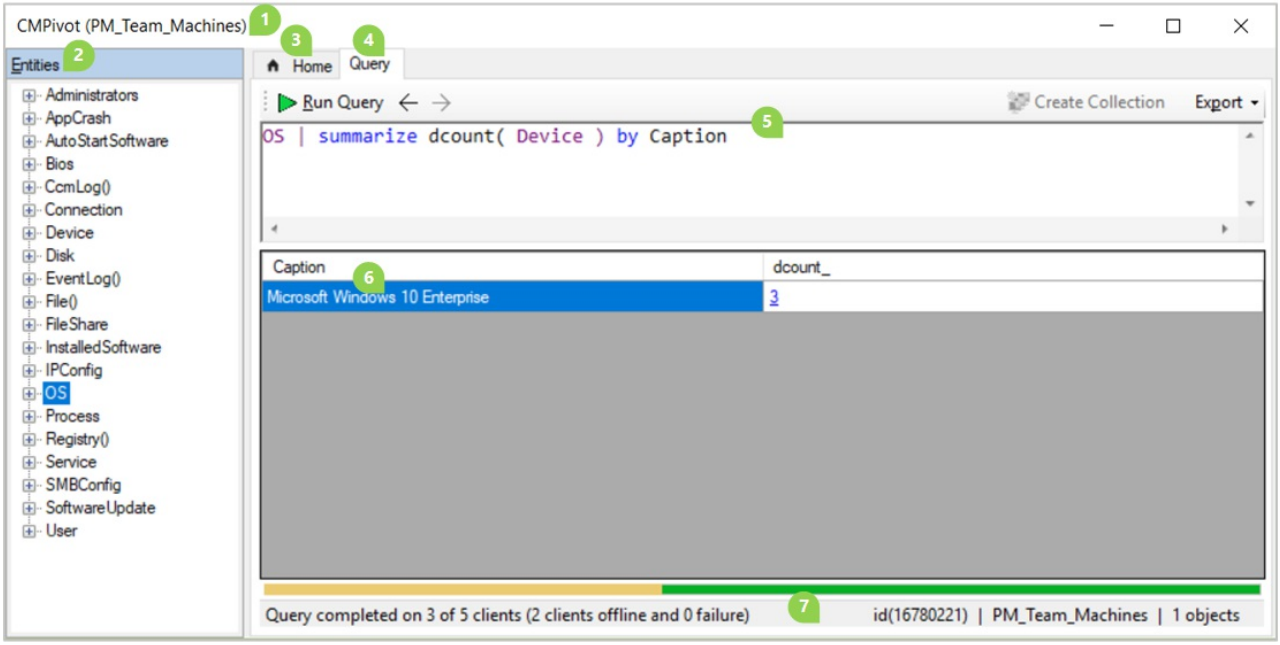
2. The interface provides further information about using the tool.

   - Manually enter query strings at the top, or click the links in the in-line documentation.
   - Click one of the **Entities** to add it to the query string.
   - The links for **Table Operators**, **Aggregation Functions**, and **Scalar Functions** open language reference documentation in the web browser. CMPivot uses the Kusto Query Language (KQL).

3. Keep the CMPivot window open to view results from clients. When you close the CMPivot window, the session is complete.

   > **NOTE**
   > If the query has been sent, then clients still send a state message response to the server.

How to use CMPivot



The CMPivot window contains the following elements:

1. The collection that CMPivot currently targets is in the title bar at the top, and the status bar at the bottom of the window. For example, "PM_Team_Machines" in the above screenshot.

2. The pane on the left lists the **Entities** that are available on clients. Some entities rely upon WMI while others use PowerShell to get data from clients.

   - Right-click an entity for the following actions:

     - **Insert**: Add the entity to the query at the current cursor position. The query doesn't automatically run. This action is the default when you double-click an entity. Use this action when building a query.

     - **Query all**: Run a query for this entity including all properties. Use this action to quickly query for a single entity.

     - **Query by device**: Run a query for this entity and group the results. For example, `Disk | summarize dcount( Device ) by Name`

   - Expand an entity to see specific properties available for each entity. Double-click a property to add it to the query at the current cursor position.

3. The **Home** tab shows general information about CMPivot, including links to sample queries and supporting documentation.

4. The **Query** tab displays the query pane, results pane, and status bar. The query tab is selected in the above screenshot example.

5. The query pane is where you build or type a query to run on clients in the collection.

   - CMPivot uses a subset of the Kusto Query Language (KQL).

   - Cut, copy, or paste content in the query pane.

   - By default, this pane uses IntelliSense. For example, if you start typing `D`, IntelliSense suggests all of the entities that start with that letter. Select an option and press Tab to insert it. Type a pipe character and a space `|`, and then IntelliSense suggests all of the table operators. Insert `summarize` and type a space, and IntelliSense suggests all of the aggregation functions. For more information on these operators and functions, click the **Home** tab in CMPivot.

- The query pane also provides the following options:
  - Run the query.
  - Move backwards and forwards in the history list of queries.
  - Create a direct membership collection.
  - Export the query results to CSV or the clipboard.

6. The results pane displays the data returned by active clients for the query.
   - The available columns vary based upon the entity and the query.
   - Click a column name to sort the results by that property.
   - Right-click on any column name to group the results by the same information in that column, or sort the results.
   - Right-click on a device name to take the following additional actions on the device:
     - **Pivot to**: Query for another entity on this device.
     - **Run Script**: Launch the Run Script wizard to run an existing PowerShell script on this device. For more information, see Run a script.
     - **Remote Control**: Launch a Configuration Manager Remote Control session on this device. For more information, see How to remotely administer a Windows client computer.
     - **Resource Explorer**: Launch Configuration Manager Resource Explorer for this device. For more information, see View hardware inventory or View software inventory.
   - Right-click on any non-device cell to take the following additional actions:
     - **Copy**: Copy the text of the cell to the clipboard.
     - **Show devices with**: Query for devices with this value for this property. For example, from the results of the `OS` query, select this option on a cell in the Version row:
       ```
       OS | summarize countif( (Version == '10.0.17134') ) by Device | where (countif_ > 0)
       ```
     - **Show devices without**: Query for devices without this value for this property. For example, from the results of the `OS` query, select this option on a cell in the Version row:
       ```
       OS | summarize countif( (Version == '10.0.17134') ) by Device | where (countif_ == 0) |
       project Device
       ```
     - **Bing it**: Launch the default web browser to https://www.bing.com with this value as the query string.
   - Click any hyperlinked text to pivot the view on that specific information.
   - The results pane doesn't show more than 20,000 rows. Either adjust the query to further filter the data, or restart CMPivot on a smaller collection.

7. The status bar shows the following information (from left to right):
   - The status of the current query to the target collection. This status includes:
     - The number of active clients that completed the query (3)
     - The number of total clients (5)
     - The number of offline clients (2)
     - Any clients that returned failure (0)

For example: `Query completed on 3 of 5 clients (2 clients offline and 0 failure)`

- The ID of the client operation. For example: `id(16780221)`
- The current collection. For example: `PM_Team_Machines`
- The total number of rows in the results pane. For example, `1 objects`

Example scenarios

The following sections provide examples of how you might use CMPivot in your environment:

Example 1: Stop a running service

Your security administrator asks you to stop and disable the Computer Browser service as quickly as possible on all devices in the accounting department. You start CMPivot on a collection for all devices in accounting, and select **Query all** on the **Service** entity.

```
Service
```

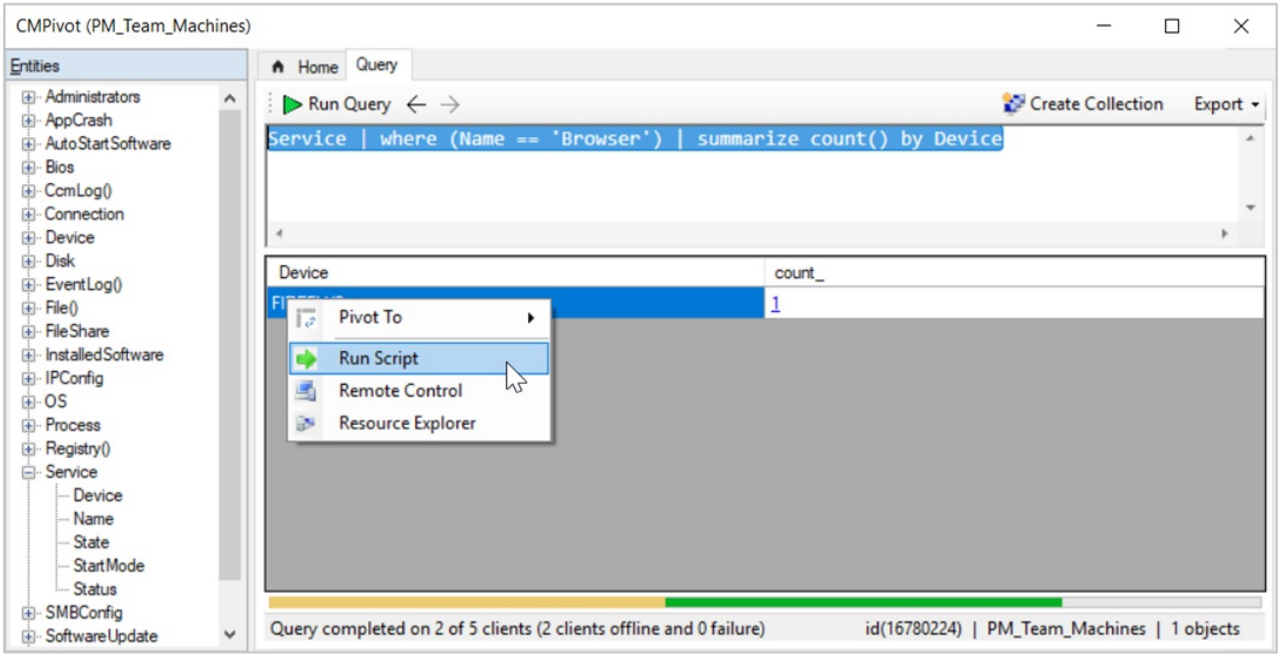
As results appear, you right-click on the **Name** column and select **Group by**.

```
Service | summarize dcount( Device ) by Name
```

In the row for the **Browser** service, you click the hyperlinked number in the **dcount_** column.

```
Service | where (Name == 'Browser') | summarize count() by Device
```

You multi-select all devices, right-click the selection, and choose **Run Script**. This action launches the Run Script wizard, from which you run an existing script you have for stopping and disabling a service. With CMPivot you quickly respond to the security incident for all active computers, viewing results in the Run Script wizard. You then followup to create a configuration baseline to remediate other computers in the collection as they become active in the future.



Example 2: Proactively resolve application failures

To be proactive with operational maintenance, once a week you run CMPivot against a collection of servers that you manage, and select **Query all** on the **AppCrash** entity. You right-click the **FileName** column and select **Sort Ascending**. One device returns seven results for sqlsqm.exe with a timestamp about 03:00 every day. You select the file name in one of the rows, right-click it, and select **Bing It**. Browsing the search results in the web browser, you find a Microsoft support article for this issue with more information and resolution.

Example 3: BIOS version

To mitigate speculative execution side channel vulnerabilities, one of the requirements is to update the system BIOS. You start with a query for the **BIOS** entity. You then **Group by** the **Version** property. Then right-click a specific value, such as "LENOVO - 1140", and select **Show devices with**.

```
Bios | summarize countif( (Version == 'LENOVO - 1140') ) by Device | where (countif_ > 0)
```

Example 4: Free disk space

You need to temporarily store a large file on a network file server, but aren't sure which one has enough capacity. Start CMPivot against a collection of file servers, and query the **Disk** entity. Modify the query for CMPivot to quickly return a list of active servers with real-time storage data:

```
Disk | where (Description == 'Local Fixed Disk') | where isnotnull( FreeSpace ) | order by FreeSpace asc
```

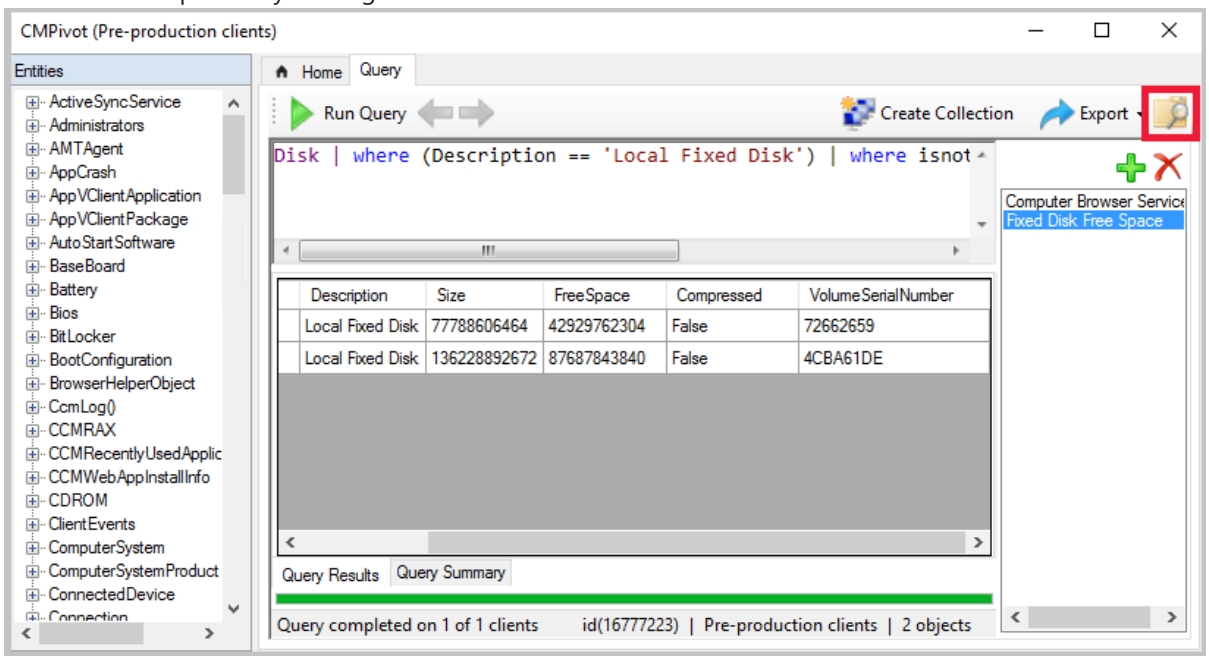
CMPivot starting in version 1810

CMPivot includes the following improvements starting in Configuration Manager version 1810:

- CMPivot utility and performance
- Scalar functions
- Rendering visualizations
- Hardware inventory
- Scalar operators
- Query summary
- Audit status messages

CMPivot utility and performance

- CMPivot will return up to 100,000 cells rather than 20,000 rows.
  - If the entity has 5 properties, meaning 5 columns, up to 20,000 rows will be shown.
  - For an entity with 10 properties, up to 10,000 rows will be shown.
  - The total data shown will be less than or equal to 100,000 cells.
- On the Query Summary tab, select the count of Failed or Offline devices, and then select the option to **Create Collection**. This option makes it easy to target those devices with a remediation deployment.
- Save **Favorite** queries by clicking the folder icon.



- Clients updated to the 1810 version return output less than 80 KB to the site over a fast communication

channel.

  - This change increases the performance of viewing script or query output.
  - If the script or query output is greater than 80 KB, the client sends the data via a state message.
  - If the client isn't updated to the 1810 client version, it continues to use state messages.
- You may see the following error when you start CMPivot: **You can't use CMPivot right now due to an incompatible script version. This issue may be because the hierarchy is in the process of upgrading a site. Wait until the upgrade is complete and then try again.**
  - If you see this message, it could mean:
    - The security scope isn't set up properly.
    - There are issues with Upgrade in the process.
    - The underlying CMPivot script is incompatible.

Scalar functions

CMPivot supports the following scalar functions:

- **ago()**: Subtracts the given timespan from the current UTC clock time
- **datetime_diff()**: Calculates the calendar difference between two datetime values
- **now()**: Returns the current UTC clock time
- **bin()**: Rounds values down to an integer multiple of a given bin size

> **NOTE**
> The datetime data type represents an instant in time, typically expressed as a date and time of day. Time values are measured in 1-second units. A datetime value is always in the UTC time zone. Always express date time literals in ISO 8601 format, for example, `yyyy-mm-dd HH:MM:ss`

Examples

- `datetime(2015-12-31 23:59:59.9)`: A specific date time literal
- `now()`: The current time
- `ago(1d)`: The current time minus one day

Rendering visualizations

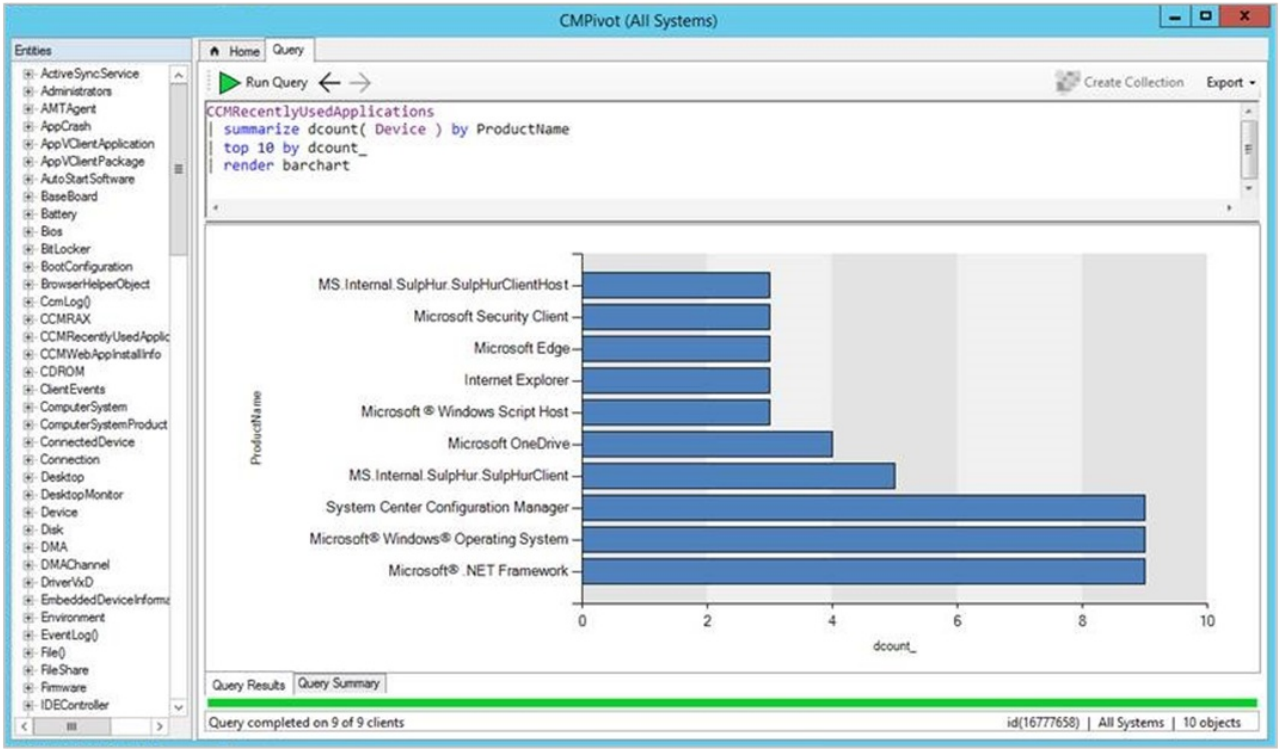
CMPivot now includes basic support for the KQL render operator. This support includes the following types:

- **barchart**: First column is x-axis, and can be text, datetime or numeric. The second columns must be numeric and is displayed as a horizontal strip.
- **columnchart**: Like barchart, with vertical strips instead of horizontal strips.
- **piechart**: First column is color-axis, second column is numeric.
- **timechart**: Line graph. First column is x-axis, and should be datetime. Second column is y-axis.

Example: bar chart

The following query renders the most recently used applications as a bar chart:

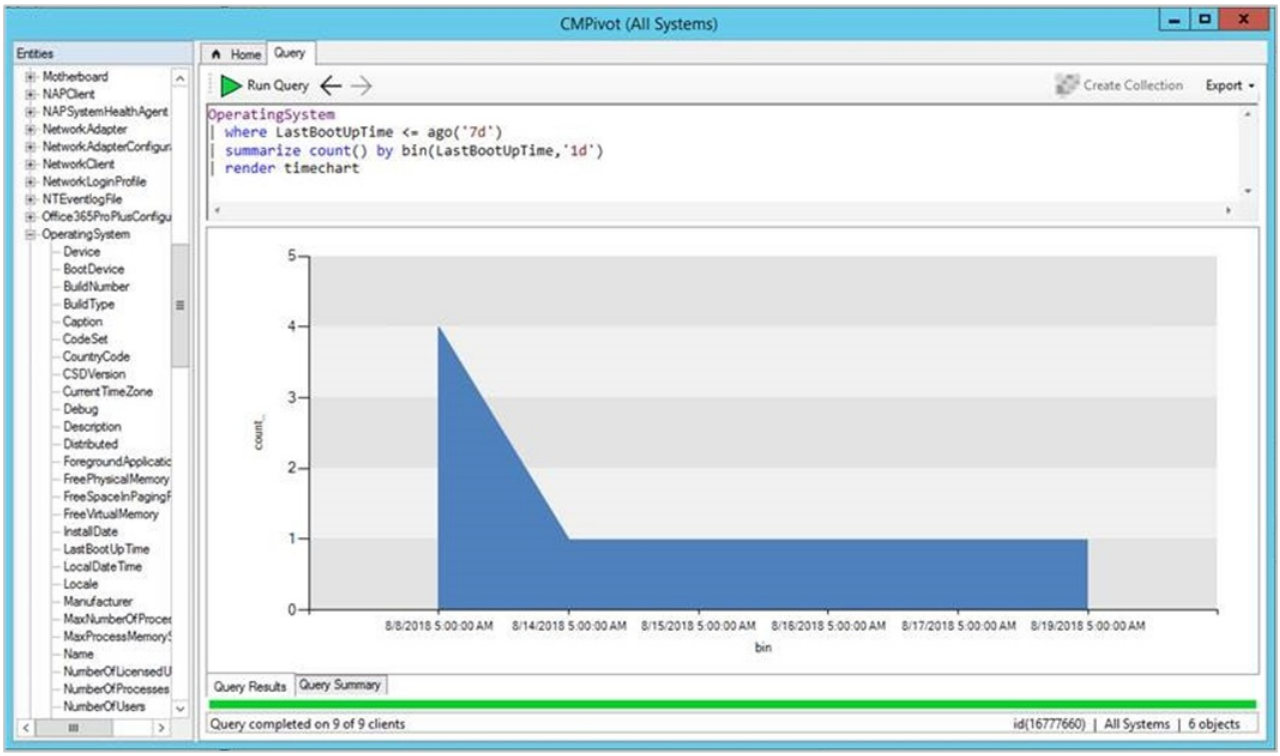
```
CCMRecentlyUsedApplications
| summarize dcount( Device ) by ProductName
| top 10 by dcount_
| render barchart
```



Example: time chart

To render time charts, use the new **bin()** operator to group events in time. The following query shows when devices have started in the last seven days:

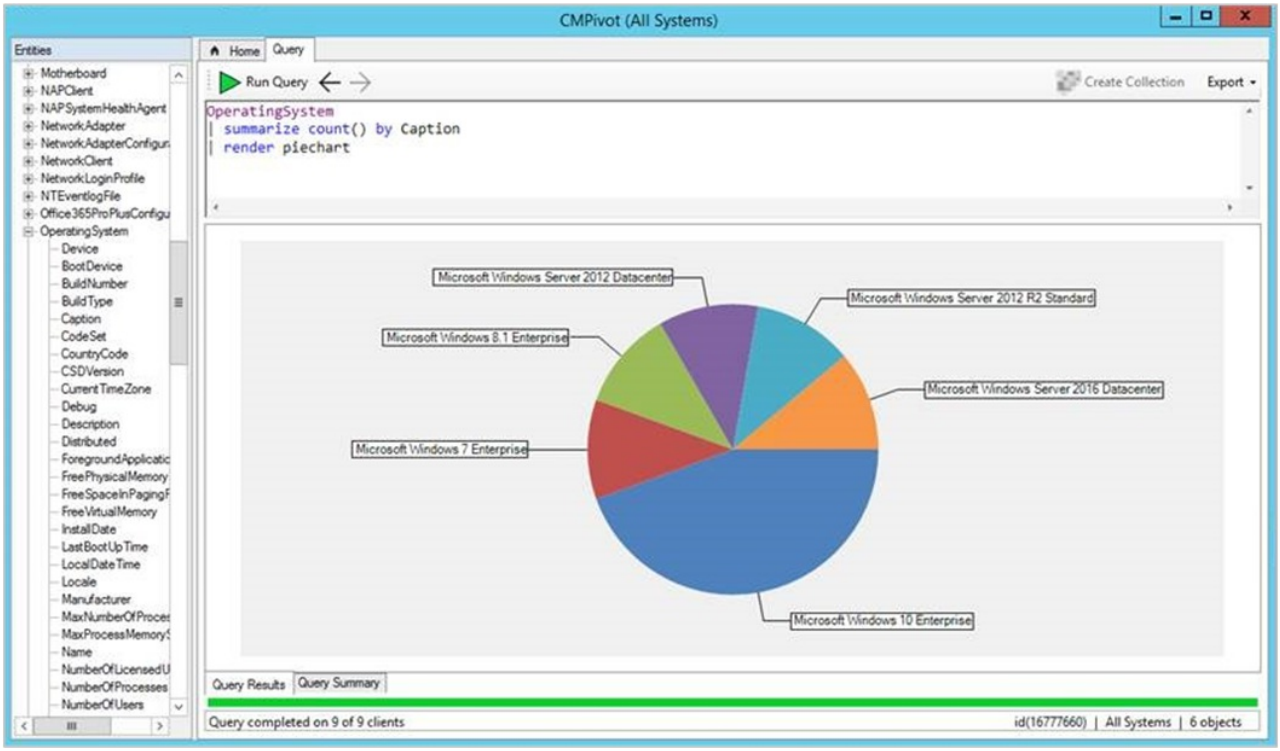
```
OperatingSystem
| where LastBootUpTime <= ago(7d)
| summarize count() by bin(LastBootUpTime,1d)
| render timechart
```



Example: pie chart

The following query displays all OS versions in a pie chart:

```
OperatingSystem
| summarize count() by Caption
| render piechart
```



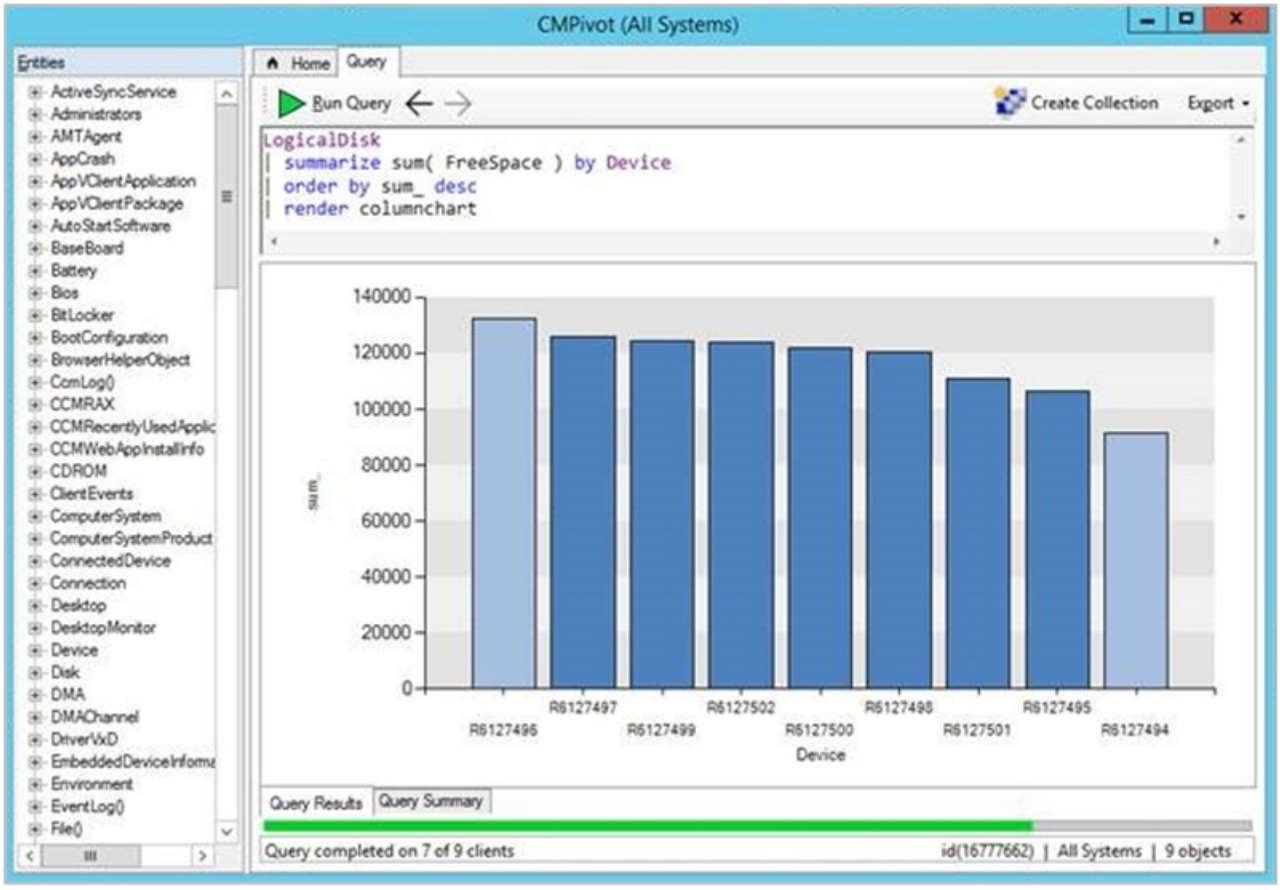
Hardware inventory

Use CMPivot to query any hardware inventory class. These classes include any custom extensions you make to hardware inventory. CMPivot immediately returns cached results from the last hardware inventory scan stored in the site database. At the same time, it updates the results if necessary with live data from any online clients.

The color saturation of the data in the results table or chart indicates if the data is live or cached. For example, dark blue is real-time data from an online client. Light blue is cached data.

Example

```
LogicalDisk
| summarize sum( FreeSpace ) by Device
| order by sum_ desc
| render columnchart
```



Limitations

- The following hardware inventory entities aren't supported:
  - Array properties, for example IP address
  - Real32/Real64
  - Embedded object properties
- Inventory entity names must begin with a character
- You can't overwrite the built-in entities by creating an inventory entity of the same name

Scalar operators

CMPivot includes the following scalar operators:

> **NOTE**
> - LHS: string to the left of the operator
> - RHS: string to the right of the operator

OPERATOR	DESCRIPTION	EXAMPLE (YIELDS TRUE)
==	Equals	`"aBc" == "aBc"`
!=	Not equals	`"abc" != "ABC"`
like	LHS contains a match for RHS	`"FabriKam" like "%Brik%"`
!like	LHS doesn't contain a match for RHS	`"Fabrikam" !like "%xyz%"`
contains	RHS occurs as a subsequence of LHS	`"FabriKam" contains "BRik"`

OPERATOR	DESCRIPTION	EXAMPLE (YIELDS TRUE)
!contains	RHS doesn't occur in LHS	`"Fabrikam" !contains "xyz"`
startswith	RHS is an initial subsequence of LHS	`"Fabrikam" startswith "fab"`
!startswith	RHS isn't an initial subsequence of LHS	`"Fabrikam" !startswith "kam"`
endswith	RHS is a closing subsequence of LHS	`"Fabrikam" endswith "Kam"`
!endswith	RHS isn't a closing subsequence of LHS	`"Fabrikam" !endswith "brik"`

Query summary

Select the **Query Summary** tab at the bottom of the CMPivot window. This status helps you identify clients that are offline, or troubleshoot errors that may occur. Select a value in the Count column to open a list of specific devices with that status.

For example, select the count of devices with a Failure status. See the specific error message, and export a list of these devices. If the error is that a specific cmdlet isn't recognized, create a collection from the exported device list to deploy a Windows PowerShell update.

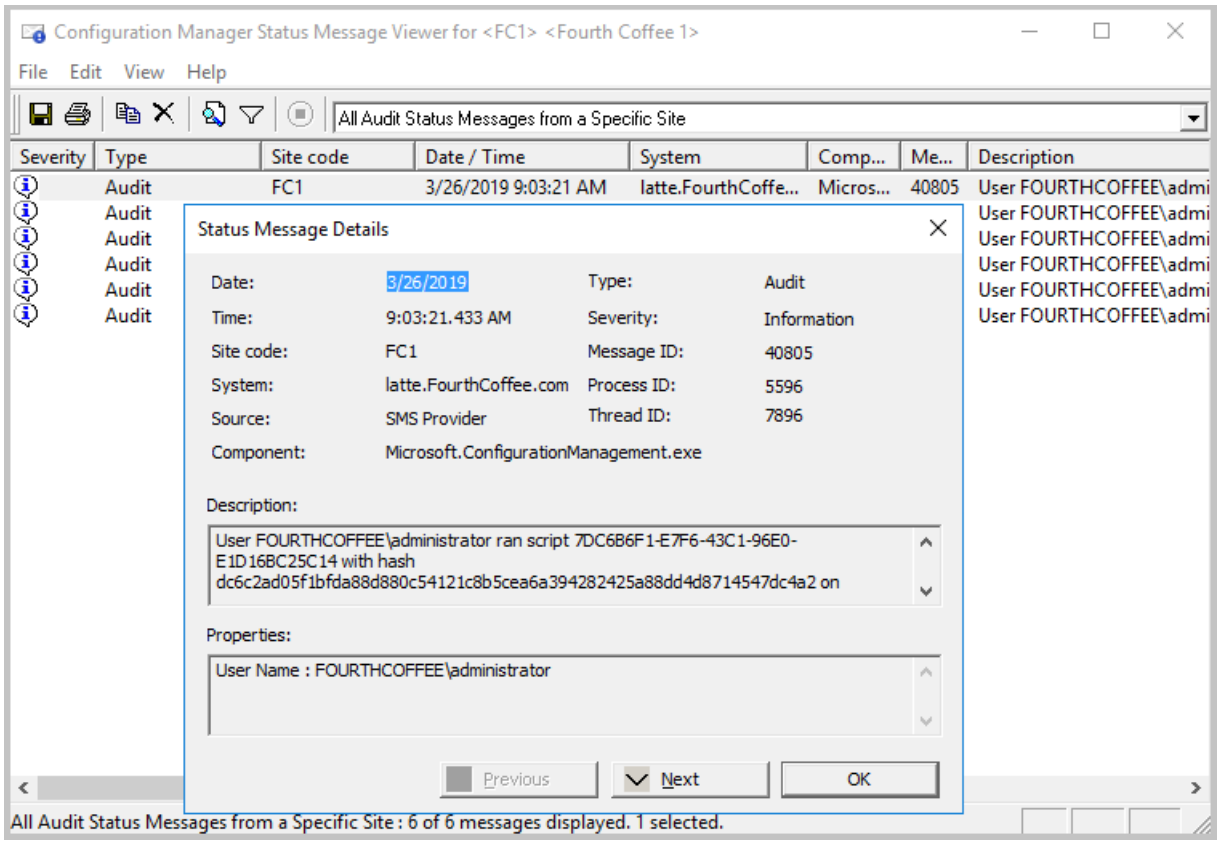
CMPivot audit status messages

Starting in version 1810, when you run CMPivot, an audit status message is created with **MessageID 40805**. You can view the status messages by going to **Monitoring** > **System Status** > **Status Message Queries**. You can run **All Audit status Messages for a Specific User**, **All Audit status Messages for a Specific Site**, or create your own status message query.

The following format is used for the message:

MessageId 40805: User <UserName> ran script <Script-Guid> with hash <Script-Hash> on collection <Collection-ID>.

- 7DC6B6F1-E7F6-43C1-96E0-E1D16BC25C14 is the Script-Guid for CMPivot.
- The Script-Hash can be seen in the client's scripts.log file.
- You can also see the hash stored in the client's script score. The filename on the client is <Script-Guid>_<Script-Hash>.
  - Example file name: C:\Windows\CCM\ScriptStore\7DC6B6F1-E7F6-43C1-96E0-E1D16BC25C14_abc1d23e45678901fabc123d456ce789fa1b2cd3e456789123fab4c56789d0123.ps



CMPivot starting in version 1902

Starting in Configuration Manager version 1902, you can run CMPivot from the central administration site (CAS) in a hierarchy. The primary site still handles the communication to the client. When running CMPivot from the central administration site, it communicates with the primary site over the high-speed message subscription channel. This communication doesn't rely upon standard SQL replication between sites.

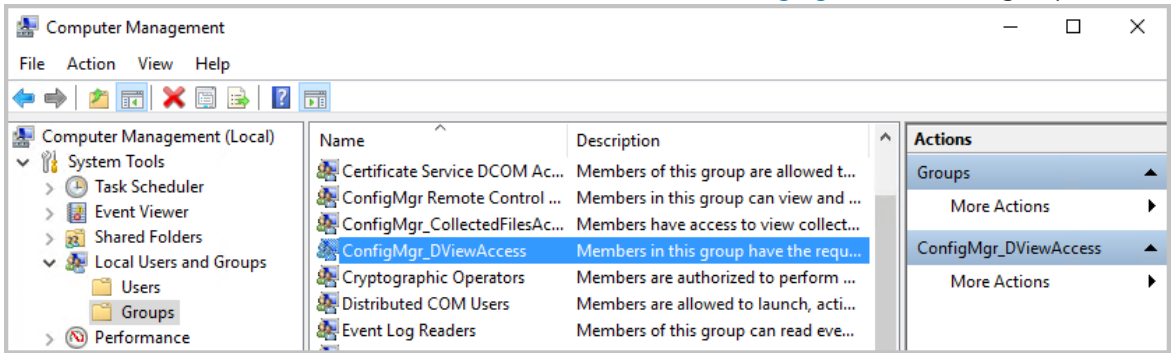
Running CMPivot on the CAS will require additional permissions when SQL or the provider aren't on the same machine or in the case of SQL Always On configuration. With these remote configurations, you have a "double hop scenario" for CMPivot.

To get CMPivot to work on the CAS in such a "double hop scenario", you can define constrained delegation. To understand the security implications of this configuration, read the Kerberos constrained delegation article. If you have more than one remote configuration such as SQL or SMS Provider being colocated with the CAS or not, you may require a combination of permission settings. Below are the steps that you need to take:

CAS has a remote SQL server

1. Go to each primary site's SQL server.

   a. Add the CAS remote SQL server and the CAS site server to the Configmgr_DviewAccess group.

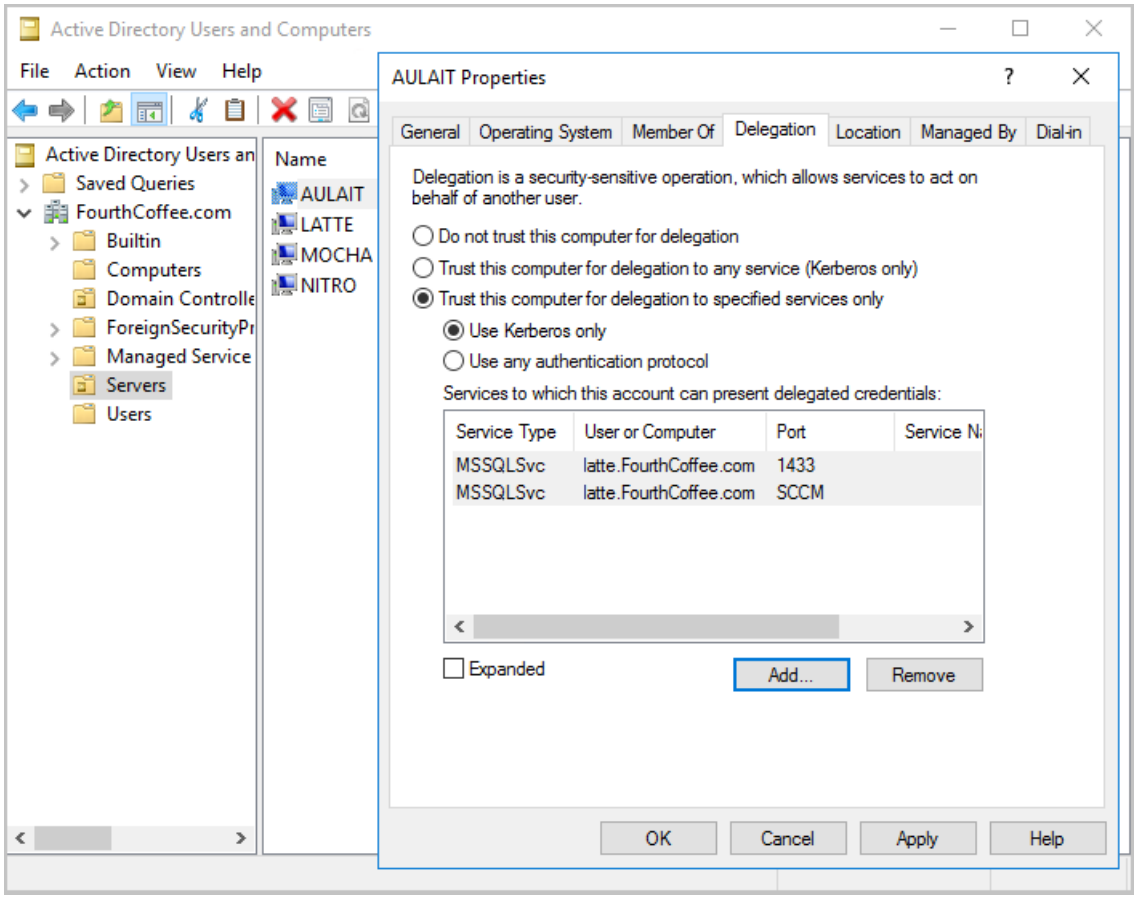


2. Go to Active Directory Users and Computers.

   a. For each primary site server, right click and select **Properties**.

a. In the delegation tab, choose the third option, **Trust this computer for delegation to specified services only**.
b. Choose **Use Kerberos only**.
c. Add the CAS's SQL server service with port and instance.
d. Make sure these changes align with your company security policy!

b. For the CAS site, right click and select **Properties**.
a. In the delegation tab, choose the third option, **Trust this computer for delegation to specified services only**.
b. Choose **Use Kerberos only**.
c. Add each primary site's SQL server service with port and instance.
d. Make sure these changes align with your company security policy!



CAS has a remote provider

1. Go to each primary site's SQL server.
   a. Add the CAS provider machine account and the CAS site server to the Configmgr_DviewAccess group.
2. Go to Active Directory Users and Computers.
   a. Select the CAS provider machine, right click and select **Properties**.
      a. In the delegation tab, choose the third option, **Trust this computer for delegation to specified services only**.
      b. Choose **Use Kerberos only**.
      c. Add each primary site's SQL server service with port and instance.
      d. Make sure these changes align with your company security policy!
   b. Select the CAS site server, right click and select **Properties**.
      a. In the delegation tab, choose the third option, **Trust this computer for delegation to specified services only**.
      b. Choose **Use Kerberos only**.
      c. Add each primary site's SQL server service with port and instance.

    d. Make sure these changes align with your company security policy!
3. Restart the CAS remote provider machine.

SQL Always On

1. Go to each primary site's SQL server.
    a. Add the CAS site server to the Configmgr_DviewAccess group.
2. Go to Active Directory Users and Computers.
    a. For each primary site server, right click and select **Properties**.
        a. In the delegation tab, choose the third option, **Trust this computer for delegation to specified services only**.
        b. Choose **Use Kerberos only**.
        c. Add the CAS's SQL server service accounts for the SQL nodes with port and instance.
        d. Make sure these changes align with your company security policy!
    b. Select the CAS site server, right click and select **Properties**.
        a. In the delegation tab, choose the third option, **Trust this computer for delegation to specified services only**.
        b. Choose **Use Kerberos only**.
        c. Add each primary site's SQL server service with port and instance.
        d. Make sure these changes align with your company security policy!
3. Make sure the SPN is published for the CAS SQL listener name and each primary SQL listener name.
4. Restart the primary SQL servers.
5. Restart the CAS site server and the CAS SQL servers.

CMPivot starting in version 1906

Starting in version 1906, the following items were added to CMPivot:

- Joins, additional operators, and aggregators
- Added CMPivot permissions to the Security Administrator role
- CMPivot standalone was added as a **pre-release feature**

Add joins, additional operators, and aggregators in CMPivot

You now have additional arithmetic operators, aggregators, and the ability to add query joins such as using Registry and File together. The following items have been added:

Table operators

TABLE OPERATORS	DESCRIPTION
join	Merge the rows of two tables to form a new table by matching row for the same device
render	Renders results as graphical output

The render operator already exists in CMPivot. Support for multiple series and the **with** statement were added. For more information, see the examples section and Kusto's join operator article.

Limitations for joins

1. The join column is always implicitly done on the **Device** field.
2. You can use a maximum of 5 joins per query.
3. You can use a maximum of 64 combined columns.

Scalar operators

OPERATOR	DESCRIPTION	EXAMPLE
+	Add	`2 + 1, now() + 1d`
-	Subtract	`2 - 1, now() - 1d`
*	Multiply	`2 * 2`
/	Divide	`2 / 1`
%	Modulo	`2 % 1`

Aggregation functions

FUNCTION	DESCRIPTION
percentile()	Returns an estimate for the specified nearest-rank percentile of the population defined by Expr
sumif()	Returns a sum of Expr for which Predicate evaluates to true

Scalar functions

FUNCTION	DESCRIPTION
case()	Evaluates a list of predicates and returns the first result expression whose predicate is satisfied
iff()	Evaluates the first argument and returns the value of either the second or third arguments depending on whether the predicate evaluated to true (second) or false (third)
indexof()	Function reports the zero-based index of the first occurrence of a specified string within input string
strcat()	Concatenates between 1 and 64 arguments
strlen()	Returns the length, in characters, of the input string
substring()	Extracts a substring from a source string starting from some index to the end of the string
tostring()	Converts input to a string operation

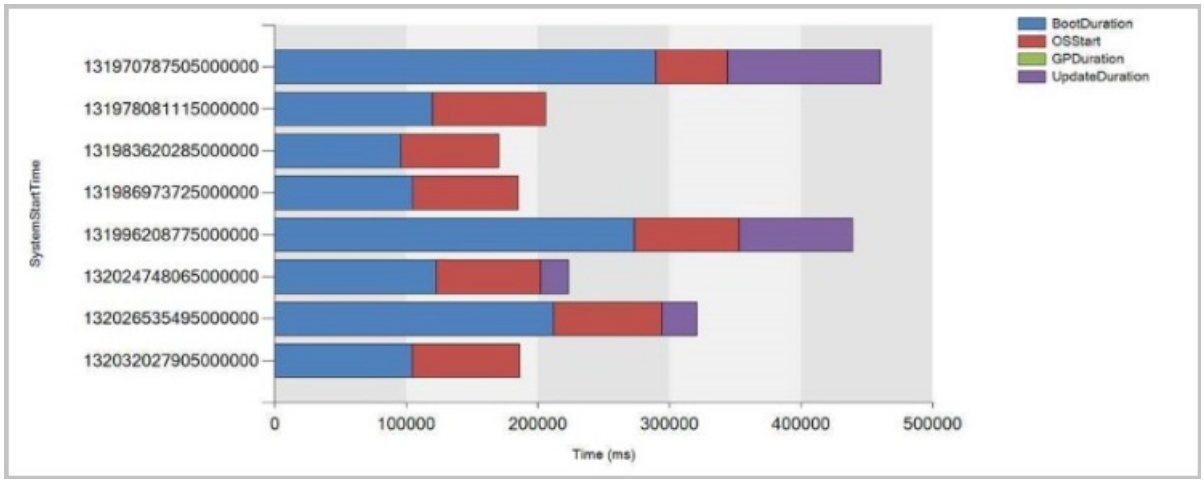
Examples

- Show device, manufacturer, model, and OSVersion:

```
ComputerSystem
| project Device, Manufacturer, Model
| join (OperatingSystem | project Device, OSVersion=Caption)
```

- Show graph of boot times for a device:

```
SystemBootData
| where Device == 'MyDevice'
| project SystemStartTime, BootDuration, OSStart=EventLogStart, GPDuration, UpdateDuration
| order by SystemStartTime desc
| render barchart with (kind=stacked, title='Boot times for MyDevice', ytitle='Time (ms)')
```



Added CMPivot permissions to the Security Administrator role

Starting in version 1906, the following permissions have been added to Configuration Manager's built-in **Security Administrator** role:

- **Read** on SMS Script
- **Run CMPivot** on Collection
- **Read** on Inventory Report

> **NOTE**
> **Run Scripts** is a super set of the **Run CMPivot** permission.

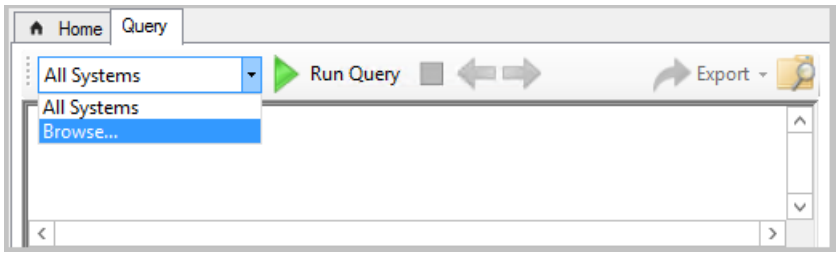
CMPivot standalone

Starting in version 1906, you can use CMPivot as a standalone app. CMPivot standalone is a pre-release feature and is only available in English. Run CMPivot outside of the Configuration Manager console to view the real-time state of devices in your environment. This change enables you to use CMPivot on a device without first installing the console.

You can share the power of CMPivot with other personas, such as helpdesk or security admins, who don't have the console installed on their computer. These other personas can use CMPivot to query Configuration Manager alongside the other tools that they traditionally use. By sharing this rich management data, you can work together to proactively solve business problems that cross roles.

Install CMPivot standalone

1. Set up the permissions needed to run CMPivot. For more information, see prerequisites. You can also use the Security Administrator role if the permissions are appropriate for the user.
2. Find the CMPivot app installer in the following path: `<site install path>\tools\CMPivot\CMPivot.msi`. You can run it from that path, or copy it to another location.
3. When you run the CMPivot standalone app, you'll be asked to connect to a site. Specify the fully qualified domain name or computer name of either the Central Administration or primary site server.
   - Each time you open CMPivot standalone you'll be prompted to connect to a site server.
4. Browse to the collection on which you want to run CMPivot, then run your query.

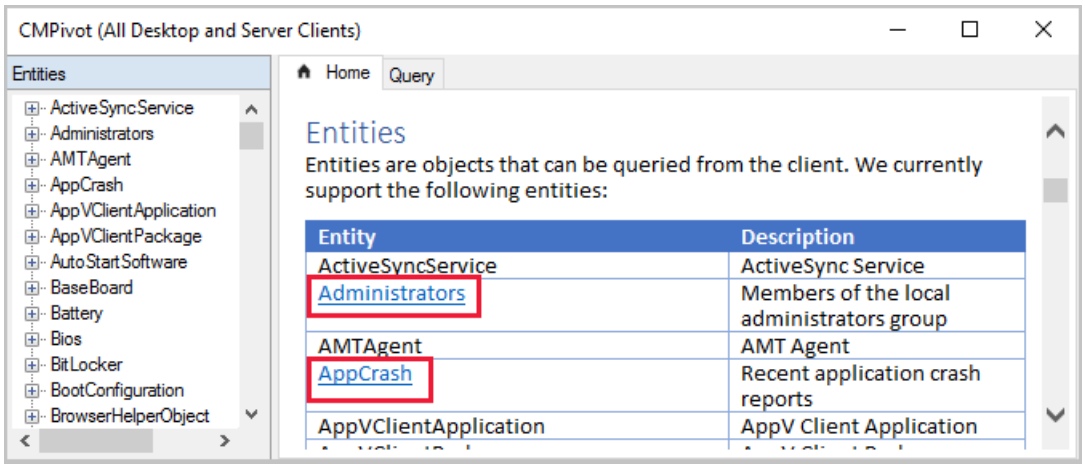


> **NOTE**
>
> Right-click actions, such as **Run Scripts** and **Resource Explorer**, aren't avilable in CMPivot standalone.

Inside CMPivot

CMPivot sends queries to clients using the Configuration Manager "fast channel". This communication channel from server to client is also used by other features such as client notification actions, client status, and Endpoint Protection. Clients return results via the similarly quick state message system. State messages are temporarily stored in the database. For more information about the ports used for client notification, see the Ports article.

The queries and the results are all just text. The entities **InstallSoftware** and **Process** return some of the largest result sets. During performance testing, the largest state message file size from one client for these queries was less than **1 KB**. Scaled to a large environment with 50,000 active clients, this one-time query would generate less than 50 MB of data across the network. All the items on the welcome page that are underlined, will return less than 1k of info per client.



Starting in Configuration Manager 1810, CMPivot can query hardware inventory data, including extended hardware inventory classes. These new entities (entities not underlined on the welcome page) may return much larger data sets, depending on how much data is defined for a given hardware inventory property. For example, the "InstalledExecutable" entity might return multiple MB of data per client, depending on the specific data you query on. Be mindful of the performance and scalability on your systems when returning larger hardware inventory data sets from larger collections using CMPivot.

A query times out after one hour. For example, a collection has 500 devices, and 450 of the clients are currently online. Those active devices receive the query and return the results almost immediately. If you leave the CMPivot window open, as the other 50 clients come online, they also receive the query, and return results.

Log files

CMPivot interactions are logged to the following log files:

Server-side:

- SmsProv.log
- BgbServer.log
- StateSys.log

Client-side:

- CcmNotificationAgent.log
- Scripts.log
- StateMessage.log

For more information, see Log files and Troubleshooting CMPivot.

Next steps

Troubleshooting CMPivot

Create and run PowerShell scripts

Troubleshooting CMPivot

9/11/2019 • 2 minutes to read • Edit Online

CMPivot is an in-console utility that now provides access to real-time state of devices in your environment. It immediately runs a query on all currently connected devices in the target collection and returns the results. Occasionally, you may find yourself needing to troubleshoot CMPivot. For example, you may see that a client sent a state message for CMPivot. However, the site server didn't process the message because it was corrupted. This article helps you understand the flow of information for CMPivot.

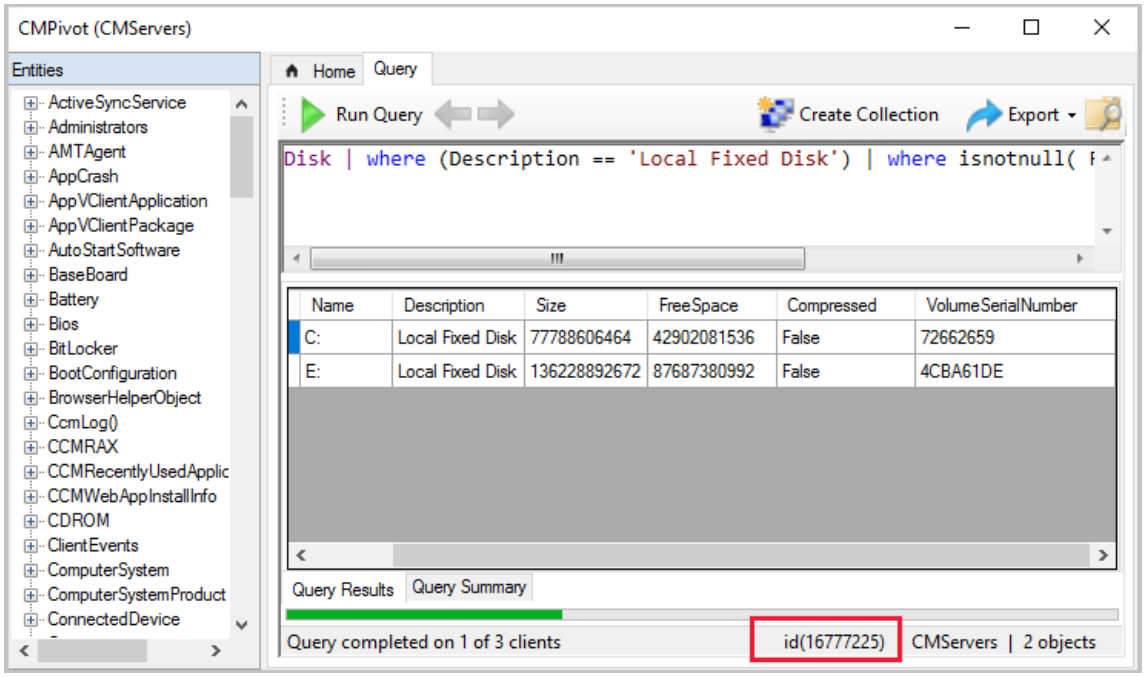
Get information from the site server

By default, the site server log files are located in C:\Program Files\Microsoft Configuration Manager\logs. This location may change depending on what was specified for your installation directory or if you offloaded items like the SMS Provider to another server.

Check the **smsprov.log** for this line:

```
Auditing: User <username> initiated client operation 135 to collection <CollectionId>.
```

Find the ID in the CMPivot window. This ID is the **ClientOperationID**.



Find the **TaskID** from the ClientAction table. The **TaskID** corresponds to the **UniqueID** in the ClientAction table.

```
select * from ClientAction where ClientOperationId=<id>
```

In the **BgbServer.log**, look for the **TaskID** you gathered from SQL. In the Bgbserver.log, it will be labeled **TaskGUID**. For example:

- Starting to send push task (PushID: 260 TaskID: 258 TaskGUID: **F8C7C37F-B42B-4C0A-B050-2BB44DF1098A** TaskType: 15 TaskParam: PFNjcmlwdEhhc2ggU2NyaXB0SGFzaEFsZz0nU0hBMjU2Jz42YzZmNDY0OGYzZjU3M2MyNTQyNWZiNTg2ZDVjYTIwNzRjNmViZmQ1NTg5MDZlMWI5NDRmYTEzNmFiMDE0ZGNjPC9TY3JpcHRlYXNoPjxTY3JpcHRQYXJhbWV0ZXJzPjxTY3JpcHRQYXJhbWV0ZXIgUGFyYW1ldGVyR3JvdXBHdWlkPSIiIFBhcmFtZX

RIckdyb3VwTmFtZT0iUEdfIiBQYXJhbWV0ZXJOYW1lPSJzZWxlY3QiIFBhcmFtZXRlckRhdGFUeXBlP
SJTeXN0ZW0uU3RyaW5nIiBQYXJhbWV0ZXJWaXNpYmlsaXR5PSIwIiBQYXJhbWV0ZXJUeXBlPSIwIiBQ
YXJhbWV0ZXJWYWx1ZT0iRGV2aWNlI2tEZXZpY2UjY05hbWUja1N0cmluZyNjTWFudWZhY3R1cmVyI2tTd
HJpbmcjY1ZlcnNpb24ja1N0cmluZyNjUmVsZWFzZURhdGUja1N0cmluZyNjU2VyaWFsTnVtYmVyI2tTdH
JpbmcjY0J1aWxkTnVtYmVyI2tTdHJpbmcjY1NNQklPU0JJT1NWZXJzaW9uI2tTdHJpbmciLz48U2NyaXB0
UGFyYW1ldGVyIFBhcmFtZXRlckdyb3VwR3VpZD0iIiBQYXJhbWV0ZXJHcm91cE5hbWU9IlBHXyIgUGFyYW
1ldGVyTmFtZT0id21pcXVlcnkiIFBhcmFtZXRlckRhdGFUeXBlPSJTeXN0ZW0uU3RyaW5nIiBQYXJhbWV0ZX
JWaXNpYmlsaXR5PSIwIiBQYXJhbWV0ZXJUeXBlPSIwIiBQYXJhbWV0ZXJWYWx1ZT0iU0VMRUNUI3NOYW1lI2N
NYW51ZmFjdHVyZXIjY1ZlcnNpb24jY1JlbGVhc2VEYXRlI2NTZXJpYWxOdW1iZXIjY0J1aWxkTnVtYmVyI2
NTTUJJT1NCSU9TVmVyc2lvbiNzRlJPTSNzV2luMzJfQmlvcyIvPjwvU2NyaXB0UGFyYW1ldGVycz48UGFyYW
1ldGVyR3JvdXBIYXNoIFBhcmFtZXRlckhhc2hBbGc9J1NIQTI1NicOTE5NmEwNzNlOTljY2U4MzEyMWE3ZmFi
ODE5N2M4M2QxMjhjNDRmNTdlMWI0NGU1NWQwNmU4YTA5NGI5ZGRkNTwvUGFyYW1ldGVyR3JvdXBIYXNoPjwvU
2NyaXB0Q29udGVudD4=-) to 5 clients with throttling (strategy: 1 param: 42) Finished sending push task (PushID:
260 TaskID: 258) to 5 clients

Client logs

Once you have the information from the site server, check the client logs. By default, the client logs are located in C:\Windows\CCM\Logs.

Check the **CcmNotificationAgent.log**. You'll find logs like the following entry:

- **Error! Bookmark not defined.**+PFNjcmlwdEhhc2ggU2NyaXB0SGFzaEFsZz0nU0hBMjU2Jz42YzZmNDY0OGYzZjU3M2MyNTQyNWZiNT
g2ZDVjYTIwNzRjNmViZmQ1NTg5MDZlMWI5NDRmYTEzNmFiMDE0ZGNjPC9TY3JpcHRlYXNoPjxTY3Jp
cHRQYXJhbWV0ZXJzPjxTY3JpcHRQYXJhbWV0ZXIgUGFyYW1ldGVyR3JvdXBBHdWlkPSIiIFBhcmFtZX
Rlckdyb3VwTmFtZT0iUEdfIiBQYXJhbWV0ZXJOYW1lPSJzZWxlY3QiIFBhcmFtZXRlckRhdGFUeXBlP
SJTeXN0ZW0uU3RyaW5nIiBQYXJhbWV0ZXJWaXNpYmlsaXR5PSIwIiBQYXJhbWV0ZXJUeXBlPSIwIiBQ
YXJhbWV0ZXJWYWx1ZT0iRGV2aWNlI2tEZXZpY2UjY05hbWUja1N0cmluZyNjTWFudWZhY3R1cmVyI2tTd
HJpbmcjY1ZlcnNpb24ja1N0cmluZyNjUmVsZWFzZURhdGUja1N0cmluZyNjU2VyaWFsTnVtYmVyI2tTdH
JpbmcjY0J1aWxkTnVtYmVyI2tTdHJpbmcjY1NNQklPU0JJT1NWZXJzaW9uI2tTdHJpbmciLz48U2NyaXB0
UGFyYW1ldGVyIFBhcmFtZXRlckdyb3VwR3VpZD0iIiBQYXJhbWV0ZXJHcm91cE5hbWU9IlBHXyIgUGFyYW
1ldGVyTmFtZT0id21pcXVlcnkiIFBhcmFtZXRlckRhdGFUeXBlPSJTeXN0ZW0uU3RyaW5nIiBQYXJhbWV0ZX
JWaXNpYmlsaXR5PSIwIiBQYXJhbWV0ZXJUeXBlPSIwIiBQYXJhbWV0ZXJWYWx1ZT0iU0VMRUNUI3NOYW1lI2N
NYW51ZmFjdHVyZXIjY1ZlcnNpb24jY1JlbGVhc2VEYXRlI2NTZXJpYWxOdW1iZXIjY0J1aWxkTnVtYmVyI2
NTTUJJT1NCSU9TVmVyc2lvbiNzRlJPTSNzV2luMzJfQmlvcyIvPjwvU2NyaXB0UGFyYW1ldGVycz48UGFyYW
1ldGVyR3JvdXBIYXNoIFBhcmFtZXRlckhhc2hBbGc9J1NIQTI1NicOTE5NmEwNzNlOTljY2U4MzEyMWE3ZmFi
ODE5N2M4M2QxMjhjNDRmNTdlMWI0NGU1NWQwNmU4YTA5NGI5ZGRkNTwvUGFyYW1ldGVyR3JvdXBIYXNoPjwvU
2NyaXB0Q29udGVudD4=-

Check **Scripts.log** for the **TaskID**. In the following example, we see **Task ID {F8C7C37F-B42B-4C0A-B050-2BB44DF1098A}**:

```
Sending script state message: 7DC6B6F1-E7F6-43C1-96E0-E1D16BC25C14 Scripts 7/3/2018 11:44:47 AM 5036 (0x13AC)
State message: Task Id {F8C7C37F-B42B-4C0A-B050-2BB44DF1098A} Scripts 7/3/2018 11:44:47 AM 5036 (0x13AC)
```

Check the **StateMessage.log**. Our example **TaskID** is near the bottom of the message next to <Param>. You should see lines similar to the one below:

```
StateMessage body: <?xml version="1.0" encoding="UTF-16"?>
<Report><ReportHeader><Identification><Machine><ClientInstalled>1</ClientInstalled><ClientType>1
</ClientType><ClientID>GUID:DBAC52C9-57E6-47D7-A8D6-E0A5A64B57E6</ClientID>
<ClientVersion>5.00.8670.1000</ClientVersion>
<NetBIOSName>R613924</NetBIOSName><CodePage>437</CodePage>
<SystemDefaultLCID>1033</SystemDefaultLCID><Priority>0</Priority></Machine></Identification>
<ReportDetails><ReportContent>State Message Data</ReportContent><ReportType>Full</ReportType>
<Date>20180703184447.673000+000</Date><Version>1.0</Version><Format>1.0</Format>
</ReportDetails></ReportHeader><ReportBody><StateMessage MessageTime="20180703184447.517000+000"><Topic
ID="7DC6B6F1-E7F6-43C1-96E0-E1D16BC25C14" Type="9003" IDType="0" User="" UserSID=""/><State ID="1" Criticality="0"/>
<StateDetails Type="1"><!
[CDATA["PAA/AHgAbQBsACAAdgBlAHIAcwBpAG8AbgA9ACIAMQAuADAAIgAgAGUAbgBjAG8AZABpAG4AZwA9ACIAdQB0AGYALQAxADYAIgA/AD4APABy
AGUAcwB1AGwAdAAgAFIAZQBzAHUAbAB0AEMAbwBkAGUAPQAiADAAIgA+ADwAZQAgAE4AYQBtAGUAPQAiAEkAbgB0AGUAbAAoAFIAKQAgAFgAZQBvAG4A
KABSACkAIABDAFAAVQAgAEUANQAtADIANgA3ADMAIAB2ADQAIABAACAAMgAuADMAMABHAEgAegAiACAATQBhAG4AdQBmAGEAYwB0AHUAcgBlAHIAPQAi
AEEAbQBlAHIAaQBjAGEAbgAgAE0AZQBnAGEAdAByAGUAbgBkAHMAIABJAG4AYwAuACIAIABWAGUAcgBzAGkAbwBuAD0AIgBWAFIAVABVAEEATAAgAC0A
IAA2ADAAMAAxADcAMAAyACIAIABSAGUAbABlAGEAcwBlAEQAYQB0AGUAPQAiADIAMAAxADcALQAwADYALQAwADIAIAAwADAAOgAwADAAOgAwADAAIgAg
AFMAZQByAGkAYQBsAE4AdQBtAGIAZQByAD0AIgAwADAAMAAwAC0AMAAwADEAOAAtADMANgA4ADIALQA0ADcAMAA4AC0ANwA2ADQAMAAtADcANgAwADAA
LQAzADMAIgAgAFMATQBCAEkATwBTAEIASQBPAFMAVgBlAHIAcwBpAG8AbgA9ACIAMAA5ADAAMAAwADcAIAAiACAALwA+ADwALwByAGUAcwB1AGwAdAA+
AA=="~~]]></StateDetails><UserParameters Flags="0" Count="2">
<Param>{F8C7C37F-B42B-4C0A-B050-2BB44DF1098A}</Param><Param>0</Param></UserParameters></StateMessage></ReportBody>
</Report>
StateMessage 7/3/2018 11:44:47 AM 5036 (0x13AC)
Successfully forwarded State Messages to the MP StateMessage 7/3/2018 11:44:47 AM 5036 (0x13AC)
```

NOTE

The above log entry in the StateSys.log is only visible when Verbose Logging is enabled for the SMS_STATE_SYSTEM component, which can be done by modifying this registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\COMPONENTS\SMS_STATE_SYSTEM\Verbose logging = 1 (Default is 0)

Review messages on the site server

Open the **statesys.log** to see if the message is received and processed. Our example **TaskID** is near the bottom of the message next to <Param>.

```
CMessageProcessor - the cmdline to DB exec dbo.spProcessStateReport N'?<?xml version="1.0" encoding="UTF-
16"?>~~<Report><ReportHeader><Identification><Machine><ClientInstalled>1</ClientInstalled><ClientType>1
</ClientType><ClientID>GUID:DBAC52C9-57E6-47D7-A8D6-E0A5A64B57E6</ClientID>
<ClientVersion>5.00.8670.1000</ClientVersion>
<NetBIOSName>R613924</NetBIOSName><CodePage>437</CodePage>
<SystemDefaultLCID>1033</SystemDefaultLCID><Priority>0</Priority></Machine></Identification>
<ReportDetails><ReportContent>State Message Data</ReportContent><ReportType>Full</ReportType>
<Date>20180703184447.673000+000</Date><Version>1.0</Version><Format>1.0</Format>
</ReportDetails></ReportHeader><ReportBody><StateMessage MessageTime="20180703184447.517000+000"><Topic
ID="7DC6B6F1-E7F6-43C1-96E0-E1D16BC25C14" Type="9003" IDType="0" User="" UserSID=""/><State ID="1" Criticality="0"/>
<StateDetails Type="1"><!
[CDATA["PAA/AHgAbQBsACAAdgBlAHIAcwBpAG8AbgA9ACIAMQAuADAAIgAgAGUAbgBjAG8AZABpAG4AZwA9ACIAdQB0AGYALQAxADYAIgA/AD4APABy
AGUAcwB1AGwAdAAgAFIAZQBzAHUAbAB0AEMAbwBkAGUAPQAiADAAIgA+ADwAZQAgAE4AYQBtAGUAPQAiAEkAbgB0AGUAbAAoAFIAKQAgAFgAZQBvAG4A
KABSACkAIABDAFAAVQAgAEUANQAtADIANgA3ADMAIAB2ADQAIABAACAAMgAuADMAMABHAEgAegAiACAATQBhAG4AdQBmAGEAYwB0AHUAcgBlAHIAPQAi
AEEAbQBlAHIAaQBjAGEAbgAgAE0AZQBnAGEAdAByAGUAbgBkAHMAIABJAG4AYwAuACIAIABWAGUAcgBzAGkAbwBuAD0AIgBWAFIAVABVAEEATAAgAC0A
IAA2ADAAMAAxADcAMAAyACIAIABSAGUAbABlAGEAcwBlAEQAYQB0AGUAPQAiADIAMAAxADcALQAwADYALQAwADIAIAAwADAAOgAwADAAOgAwADAAIgAg
AFMAZQByAGkAYQBsAE4AdQBtAGIAZQByAD0AIgAwADAAMAAwAC0AMAAwADEAOAAtADMANgA4ADIALQA0ADcAMAA4AC0ANwA2ADQAMAAtADcANgAwADAA
LQAzADMAIgAgAFMATQBCAEkATwBTAEIASQBPAFMAVgBlAHIAcwBpAG8AbgA9ACIAMAA5ADAAMAAwADcAIAAiACAALwA+ADwALwByAGUAcwB1AGwAdAA+
AA=="~~]]></StateDetails><UserParameters Flags="0" Count="2">
<Param>{F8C7C37F-B42B-4C0A-B050-2BB44DF1098A}</Param><Param>0</Param></UserParameters></StateMessage></ReportBody>
</Report>~~'
```

Check the state message inbox if you don't see that the message has been processed. The default location of the inbox is C:\Program Files\Microsoft Configuration Manager\inboxes\auth\statesys.box. The files will be in either:

- Incoming
- Corrupted
- Process

Check the monitoring view for CMPivot from SQL using the **TaskID**.

```
select * from vSMS_CMPivotStatus where TaskID='{F8C7C37F-B42B-4C0A-B050-2BB44DF1098A}'
```

Next steps

Using CMPivot

Create and run PowerShell scripts

Maintenance tasks for System Center Configuration Manager

7/26/2019 • 7 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

System Center Configuration Manager sites and hierarchies require regular maintenance and monitoring to provide services effectively and continuously. Regular maintenance ensures that the hardware, software, and Configuration Manager database continue to function correctly and efficiently. Optimal performance greatly reduces the risk of failure.

To set up Alerts and use the Status System to monitor the health of Configuration Manager, see Use alerts and the status system for System Center Configuration Manager.

Maintenance tasks

Regular maintenance is important to ensure correct site operations. Keep a maintenance log to document maintenance dates, who did maintenance, and any maintenance-related comments about the tasks. To maintain your site, consider daily or weekly maintenance. Some tasks might require a different schedule. Common maintenance can include both the built-in maintenance tasks and other tasks like account maintenance to maintain compliance with your company policies.

Use the following information as a guide to help you plan when to do different maintenance tasks. Use these lists as a starting point, and add tasks that you might require.

Daily Tasks

The following are maintenance tasks that you might consider for on a daily schedule:

- Check that predefined maintenance tasks that are scheduled to run daily are running successfully.
- Check the Configuration Manager database status.
- Check site server status.
- Check Configuration Manager site system inboxes for file backlogs.
- Check site systems status.
- Check the operating system event logs from the site systems.
- Check the SQL Server error log from the site database computer.
- Check system performance.
- Check Configuration Manager alerts.

Weekly Tasks

The following are maintenance tasks that you might consider for a weekly schedule:

- Check that predefined maintenance tasks that are scheduled to run weekly are running successfully.
- Delete unnecessary files from site systems.
- Produce and distribute end-user reports if necessary.

- Back up application, security, and system event logs and clear them.
- Check the site database size and verify there's enough available disk space on the site database server so that the site database can grow.
- Do SQL Server database maintenance on the site database according to your SQL Server maintenance plan.
- Check available disk space on all site systems.
- Run disk defragmentation tools on all site systems.

Periodic Tasks

Some tasks that don't require daily or weekly maintenance are important to ensure overall site health. These tasks also ensure that security and disaster recovery plans are up-to-date. The following are maintenance tasks that you might consider for a more periodic schedule than the daily or weekly tasks:

- Change accounts and passwords, if it's necessary, according to your security plan.
- Review the maintenance plan to check that scheduled maintenance tasks are scheduled correctly and effectively depending on configured site settings.
- Review the Configuration Manager hierarchy design for any required changes.
- Check network performance to ensure that changes haven't been made that affect site operations.
- Check that Active Directory settings that affect site operations haven't changed. For example, check that subnets that are assigned to Active Directory sites and that are used as boundaries for Configuration Manager site haven't changed.
- Review your disaster recovery plan for any required changes.
- Do a site recovery according to the disaster recovery plan in a test lab by using a backup copy of the most recent backup that the Backup Site Server maintenance task created.
- Check hardware for any errors or for available hardware updates.
- Check the overall health of the site.

Maintain the operational health of your site database

While your Configuration Manager site and hierarchy do the tasks that you schedule and set up, site components continually add data to the Configuration Manager database. As the amount of data grows, database performance and the free storage space in the database decline. You can set up site maintenance tasks to remove aged data that you no longer require.

Configuration Manager provides predefined maintenance tasks that you can use to maintain the health of the Configuration Manager database. Not all maintenance tasks are available at each site, by default. Several tasks are enabled while some aren't, and all support a schedule that you can set up.

Most maintenance tasks periodically remove out-of-date data from the Configuration Manager database. Reducing the size of the database by removing unnecessary data improves the performance and the integrity of the database, which increases the efficiency of the site and hierarchy. Other tasks, like **Rebuild Indexes**, help maintain the database efficiency. Other tasks, like the **Backup Site Server** task, help you prepare for disaster recovery.

IMPORTANT

When you plan the schedule of any task that deletes data, consider the use of that data across the hierarchy. When a task that deletes data runs at a site, the information is removed from the Configuration Manager database, and this change replicates to all sites in the hierarchy. This deletion can affect other tasks that rely on that data. For example, at the central administration site, you might set up Discovery to run one time per month to identify non-client computers. You plan to install the Configuration Manager client to these computers within two weeks of their discovery. However, at one site in the hierarchy, an admin sets up the Delete Aged Discovery Data task to run every seven days. The result is that seven days after non-client computers are discovered, they are deleted from the Configuration Manager database. Back at the central administration site, you prepare to push install the Configuration Manager client to these new computers on day 10. However, because the Delete Aged Discovery Data task has recently run and deleted data that's seven days or older, the recently discovered computers are no longer available in the database.

After you install a Configuration Manager site, review the available maintenance tasks and enable those tasks that your operations require. Review the default schedule of each task, and when necessary, set up the schedule to fine-tune the maintenance task to fit your hierarchy and environment. Although the default schedule of each task should suit most environments, monitor the performance of your sites and database and expect to fine-tune tasks to increase your deployment's efficiency. Plan to periodically review the site and database performance and reconfigure maintenance tasks and their schedules to maintain that efficiency.

Set up maintenance tasks

Each Configuration Manager site supports maintenance tasks that help maintain the operational efficiency of the site database. By default, several maintenance tasks are enabled in each site, and all tasks support independent schedules. Maintenance tasks are set up individually for each site and apply to the database at that site. However, some tasks, like **Delete Aged Discovery Data**, affect information that is available in all sites in a hierarchy.

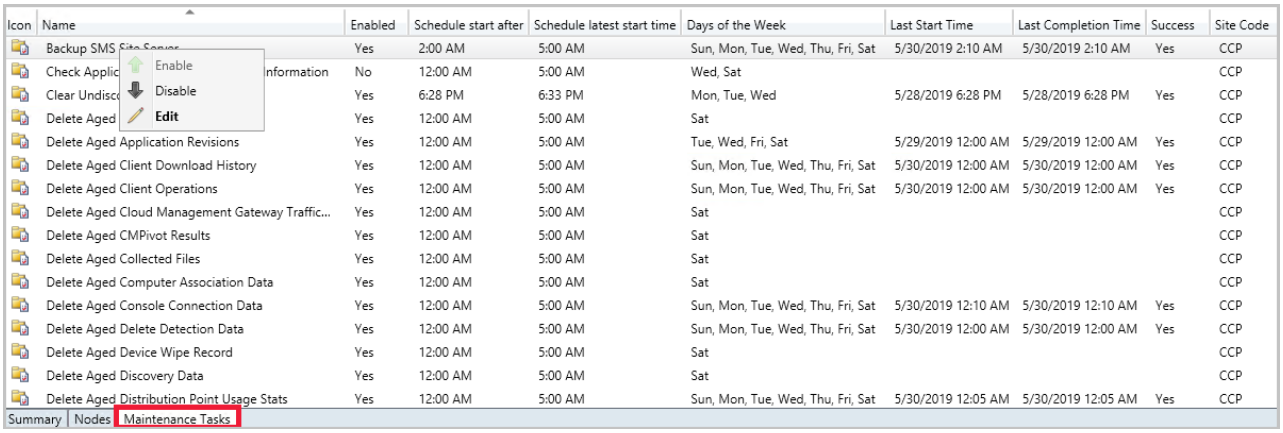
Only the maintenance tasks that you can set up at a site are displayed in the Configuration Manager console. For a complete list of maintenance tasks by site type, see Reference for maintenance tasks for System Center Configuration Manager.

Use the following procedure to help you set up the common settings of maintenance tasks.

To set up maintenance tasks for Configuration Manager version 1906

Starting in version 1906, site server maintenance tasks can now be viewed, edited, and monitored from their own tab on the details view of a site server. You can still edit maintenance tasks by choosing **Site Maintenance** in the **Settings** group like you did in previous Configuration Manager versions.

1. In the Configuration Manager console, go to **Administration** > **Site Configuration** >**Sites**.
2. Select a site from your list, then click on the **Maintenance Tasks** tab in the detail panel.
3. Only tasks that are available at the selected site are displayed. Right-click one of the maintenance tasks and choose one of the following options:
   - **Enable** - Turn on the task.
   - **Disable** - Turn off the task.
   - **Edit** - Edit the task schedule or its properties.



The **Maintenance Tasks** tab gives you information such as:

- If the task is enabled
- The task schedule
- Last start time
- Last completion time
- If the task completed successfully

To set up maintenance tasks for Configuration Manager version 1902 and prior

1. In the Configuration Manager console, go to **Administration** > **Site Configuration** >**Sites**.
2. Choose the site that has the maintenance task that you want to set up.
3. On the **Home** tab, in the **Settings** group, choose **Site Maintenance**, and then choose the maintenance task that you want to set up. Only tasks that are available at the selected site are displayed.
4. To set up the task, choose **Edit**. Ensure the **Enable this task** check box is checked, and set up a schedule for when the task runs. If the task also deletes aged data, set up the age of data that will be deleted from the database when the task runs. Choose **OK** to close the task **Properties**.

   > **NOTE**
   > For **Delete Aged Status Messages**, you set up the age of data to delete when you set up status filter rules.

5. To enable or disable the task without editing the task properties, choose the **Enable** or **Disable** button. The button label changes depending on the current configuration of the task.
6. When you're finished configuring the maintenance tasks, choose **OK** to finish the procedure.

Next steps

Reference for maintenance tasks

Reference for maintenance tasks in Configuration Manager

9/5/2019 • 14 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article lists the details for each of the Configuration Manager site maintenance tasks. Each entry specifies the site types where the task is available, and whether it's enabled by default.

For more information, see Set up maintenance tasks.

Tasks

Backup Site Server

Use this task to create a backup of your critical information to restore a site and the Configuration Manager database. For more information, see Back up a Configuration Manager site.

Central administration site	Enabled
Primary site	Not enabled
Secondary site	Not available

Check Application Title with Inventory Information

Use this task to maintain consistency of software titles between software inventory and the Asset Intelligence catalog. For more information, see Introduction to Asset Intelligence.

Central administration site	Enabled
Primary site	Not available
Secondary site	Not available

Clear Undiscovered Clients

> **TIP**
> You may also see this task in the console named **Clear Install Flag**.

Use this task to remove the installed flag for clients that don't submit a Heartbeat Discovery record during the **Client Rediscovery** period. The installed flag prevents automatic client push installation to a computer that might have an active Configuration Manager client.

Central administration site	Not available

Primary site	Not enabled
Secondary site	Not available

Delete Aged Application Request Data

Use this task to delete aged application requests from the database. For more information, see Create and deploy an application.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Application Revisions

Use this task to delete application revisions that are no longer referenced. For more information, see How to revise and supersede applications.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Not available

Delete Aged Client Download History

Use this task to delete historical data about the download source used by clients. The site uses download source information to populate the Client Data Sources dashboard.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Client Operations

Use this task to delete from the site database all aged data for client operations. For example, this data includes the following operations:

- Aged or expired client notifications, like download requests for machine or user policy
- Endpoint Protection, like requests by an administrative user for clients to run a scan or download updated definitions

Central administration site	Enabled
Primary site	Enabled

Secondary site	Not available

Delete Aged Client Presence History

Use this task to delete history information about the online status of clients recorded by client notification. It deletes information for clients with status that's older than the specified time. For more information, see How to monitor clients.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Not available

Delete Aged Cloud Management Gateway Traffic Data

Use this task to delete from the site database all aged data about the traffic that passes through the cloud management gateway. This data includes:

- The number of requests
- Total request bytes
- Total response bytes
- Number of failed requests
- Maximum number of concurrent requests

Central administration site	Enabled
Primary site	Enabled
Secondary site	Not available

Delete Aged CMPivot Results

Use this task to delete from the site database aged information from clients in CMPivot queries. For more information, see CMPivot for real-time data.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Collected Files

Use this task to delete from the database aged information about collected files. This task also deletes the collected files from the site server folder structure at the selected site. By default, the five most-recent copies of collected files are stored on the site server in the **Inboxes\sinv.box\FileCol** directory. For more information, see Introduction to software inventory.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Computer Association Data

Use this task to delete from the database aged OS deployment computer association data. This information is used when restoring user state during a task sequence. For more information, see Manage user state.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Console Connection Data

This task deletes data from the site database about console connections to the site.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Not available

Delete Aged Delete Detection Data

Use this task to delete aged data from the database that has been created by extraction views. It deletes old data change information used by external systems extracting data from the database.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Not available

Delete Aged Device Wipe Record

Use this task to delete from the database aged data about mobile device wipe actions. For more information, see Protect data with remote wipe, lock, or passcode reset.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Discovery Data

Use this task to delete aged discovery data from the database. This data can include records from:

- Heartbeat discovery
- Network discovery
- Active Directory discovery methods: System, User, and Group

This task also removes aged devices marked as decommissioned. When this task runs at a site, data associated with that site is deleted, and those changes replicate to other sites. For more information, see Run discovery.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Distribution Point Usage Stats

Use this task to delete from the database aged data for distribution points that has been stored longer than a specified time.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Not available

Delete Aged Enrolled Devices

Use this task to delete from the site database the aged data about mobile devices that haven't reported any information to the site for a specified time.

This task applies to devices that are enrolled with Configuration Manager on-premises MDM. For more information on these devices, see Supported operating systems for clients and devices.

Central administration site	Not available
Primary site	Not enabled
Secondary site	Not available

Delete Aged EP Health Status History Data

Use this task to delete from the database aged status information for Endpoint Protection (EP). For more information, see How to monitor Endpoint Protection.

Central administration site	Not available
Primary site	Enabled

Secondary site	Not available

Delete Aged Exchange Partnership

> **TIP**
>
> You may also see this task in the console named **Delete Aged Devices Managed by the Exchange Server Connector**.

Use this task to delete aged data about mobile devices managed by the Exchange Server connector. The site deletes this data according to the **Ignore mobile devices that are inactive for more than (days)** setting on the **Discovery** tab of the Exchange Server connector properties. For more information, see Manage mobile devices with Configuration Manager and Exchange.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Inventory History

Use this task to delete from the database inventory data that has been stored longer than a specified time. For more information, see How to use Resource Explorer to view hardware inventory.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Log Data

Use this task to delete from the database aged log data used for troubleshooting. This data isn't related to Configuration Manager component operations.

> **IMPORTANT**
>
> By default, this task runs daily at each site. At a central administration site and primary sites, the task deletes data that's older than 30 days. When you use SQL Server Express at a secondary site, make sure that this task runs daily and deletes data that's inactive for seven days.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Enabled

Delete Aged Metering Data

Use this task to delete from the database aged data for software metering that has been stored longer than a specified time. For more information, see Software metering.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Metering Summary Data

Use this task to delete from the database aged summary data for software metering that's been stored longer than a specified time. For more information, see Software metering.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Notification Server History

This task deletes aged client presence history.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Not available

Delete Aged Notification Task History

Use this task to delete from the site database information about client notification tasks. This task applies to data that hasn't been updated for a specified time. For more information, see Client notifications.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Passcode Records

Use this task at the top-level site of your hierarchy to delete aged Passcode Reset data for Android and Windows Phone devices. Passcode Reset data is encrypted, but does include the PIN for devices. By default, this task is enabled, and deletes data that is older than one day.

Central administration site	Enabled

Primary site	Enabled
Secondary site	Not available

Delete Aged Replication Data

Use this task to delete from the database aged data about database replication between Configuration Manager sites. When you change the configuration of this maintenance task, the configuration applies to each applicable site in the hierarchy. For more information, see Monitor database replication.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Enabled

Delete Aged Replication Summary Data

Use this task to delete from the site database aged replication summary data when it hasn't been updated for a specified time. For more information, see Monitor database replication.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Enabled

Delete Aged Status Messages

Use this task to delete from the database aged status message data as configured in status filter rules. For more information, see Monitor the status system of Configuration Manager.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Not available

Delete Aged Threat Data

Use this task to delete from the database aged Endpoint Protection threat data that's been stored longer than a specified time. For more information, see Endpoint Protection.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged Unknown Computers

Use this task to delete information about unknown computers from the site database when it hasn't been updated for a specified time. For more information, see Prepare for unknown computer deployments.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Aged User Device Affinity Data

Use this task to delete aged User Device Affinity data from the database. For more information, see Link users and devices with user device affinity.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Delete Duplicate System Discovery Data

Use this task to delete from the site database any duplicate records generated by system discovery.

Central administration site	Enabled
Primary site	Not available
Secondary site	Not available

Delete Expired MDM Bulk Enroll Package Records

Use this task to delete old Bulk Enrollment certificates and corresponding profiles after the enrollment certificate has expired. For more information, see Create certificate profiles.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Not available

Delete Inactive Client Discovery Data

Use this task to delete from the database discovery data for inactive clients. The site marks clients as inactive when the client is flagged as obsolete and by configurations that are made for client status.

This task operates only on resources that are Configuration Manager clients. It's different than the **Delete Aged Discovery Data** task, which deletes any aged discovery data record. When this task runs at a site, it removes the data from the database at all sites in a hierarchy. For more information, see How to configure client status.

IMPORTANT

When it's enabled, configure this task to run at an interval greater than the **Heartbeat Discovery** schedule. This configuration enables active clients to send a Heartbeat Discovery record to mark their client record as active so this task doesn't delete them.

Central administration site	Not available
Primary site	Not enabled
Secondary site	Not available

Delete Obsolete Alerts

Use this task to delete from the database expired alerts that have been stored longer than a specified time. For more information, see Use alerts and the status system.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Not available

Delete Obsolete Client Discovery Data

Use this task to delete obsolete client records from the database. A record that's marked as obsolete has usually been replaced by a newer record for the same client. The newer record becomes the client's current record. For information about discovery, see Run discovery.

IMPORTANT

When it's enabled, configure this task to run at an interval greater than the Heartbeat Discovery schedule. This configuration enables the client to send a Heartbeat Discovery record that correctly sets the obsolete status.

Central administration site	Not available
Primary site	Not enabled
Secondary site	Not available

Delete Obsolete Forest Discovery Sites and Subnets

Use this task to delete data about Active Directory sites, subnets, and domains. It removes data that the site hasn't discovered by the Active Directory Forest Discovery method in the last 30 days. This task removes the discovery data, but doesn't affect boundaries that you create from this discovery data. For more information, see Run discovery.

Central administration site	Enabled

Primary site	Enabled
Secondary site	Not available

Delete Orphaned Client Deployment State Records

Use this task to periodically purge the table that contains client deployment state information. This task cleans up records associated with obsolete or decommissioned devices.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Evaluate Collection Members

You configure the Collection Membership Evaluation as a site component. For more information, see Site components.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Monitor Keys

Use this task to monitor the integrity of the Configuration Manager database primary keys. A primary key is a column or a combination of columns that uniquely identifies one row. The key distinguishes the row from any other row in a Microsoft SQL Server database table.

Central administration site	Enabled
Primary site	Enabled
Secondary site	Not available

Rebuild Indexes

Use this task to rebuild the Configuration Manager database indexes. An index is a database structure that's created on a database table to speed up data retrieval. For example, searching an indexed column is often much faster than searching a column that isn't indexed.

To improve performance, the Configuration Manager database indexes are frequently updated to remain synchronized with the constantly changing data that's stored in the database. This task:

- Creates indexes on database columns that are at least 50 percent unique
- Drops indexes on columns that are less than 50 percent unique
- Rebuilds all existing indexes that meet the data uniqueness criteria

Central administration site	Not enabled
Primary site	Not enabled
Secondary site	Not enabled

Summarize File Usage Metering Data

Use this task to summarize the data from multiple records for software metering file usage into one general record. Data summarization can compress the amount of data that's stored in the Configuration Manager database.

To summarize software metering data and to conserve disk space in the database, use this task with the **Summarize Software Metering Monthly Usage Data** task. For more information, see Software metering.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Summarize Installed Software Data

Use this task to summarize the data for installed software from multiple records into one general record. Data summarization can compress the amount of data that's stored in the Configuration Manager database. For more information, see Introduction to software inventory.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Summarize Monthly Usage Metering Data

Use this task to summarize the data from multiple records for software metering monthly usage into one general record. Data summarization can compress the amount of data that's stored in the Configuration Manager database.

To summarize software metering data and to conserve space in the database, use this task with the **Summarize Software Metering File Usage Data** task. For more information, see Software metering.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Update Application Available Targeting

Use this task to have Configuration Manager recalculate the mapping of policy and application deployments to

resources in collections. When you deploy policy or applications to a collection, Configuration Manager creates an initial mapping between the objects that you deploy and the collection members.

These mappings are stored in a table for quick reference. When a collections membership changes, the site updates these stored mappings to reflect those changes. However, it's possible for these mappings to fall out of sync. For example, if the site fails to properly process a notification file, that change might not be reflected in a change to the mappings. This task refreshes that mapping based on current collection membership.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

Update Application Catalog Tables

Use this task to synchronize the Application Catalog website database cache with the latest application information. When you change the configuration of this maintenance task, it applies to all primary sites in the hierarchy.

Central administration site	Not available
Primary site	Enabled
Secondary site	Not available

See also

Maintenance tasks

Modify your System Center Configuration Manager infrastructure

9/5/2019 • 18 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

After you install one or more sites, you might have need to modify configurations or take actions that affect the infrastructure you have deployed.

Manage the SMS Provider

The SMS Provider (a dynamic-link library file: smsprov.dll) provides the point of administrative contact for one or more Configuration Manager consoles. When you install multiple SMS Providers, you can provide redundancy for contact points to administer your site and hierarchy.

At each Configuration Manager site, you can re-run Setup to:

- Add an additional instance of the SMS Provider (Each additional instance of the SMS Provider must be on a separate computer)
- Remove an instance of the SMS Provider (To remove the last SMS Provider for a site, you must uninstall the site)

You can monitor the installation or removal of the SMS Provider by viewing the **ConfigMgrSetup.log** in the root folder of the site server on which you run Setup.

Before modifying the SMS Provider at a site, be familiar with the information in Plan for the SMS Provider for System Center Configuration Manager.

To manage the SMS Provider configuration for a site

1. Run **Configuration Manager Setup** from **<Configuration Manager site installation folder>\BIN\X64\setup.exe**.
2. On the **Getting Started** page, select **Perform site maintenance or reset this site**, and then click **Next**
3. On the **Site Maintenance** page, select **Modify SMS Provider configuration**, and then click **Next**.
4. On the **Manage SMS Providers** page, select one of the following options and complete the wizard by using one of the following options:

   - To add an additional SMS Provider at this site:

     Select **Add a new SMS Provider**, specify the FQDN for a computer that will host the SMS Provider and does not currently host a SMS Provider, and then click **Next**.

   - To remove an SMS Provider from a server:

     Select **Uninstall the specified SMS Provider**, select the name of the computer from which you want to remove the SMS Provider, click **Next**, and then confirm the action.

> **TIP**
> To move the SMS Provider between two computers, you must install the SMS Provider to the new computer, and remove the SMS Provider from the original location. There is no dedicated option to move the SMS Provider between computers in a single process.

After the Setup Wizard finishes, the SMS Provider configuration is completed. On the **General** tab in the site **Properties** dialog box, you can verify the computers that have an SMS Provider installed for a site.

Manage the Configuration Manager console

The following are tasks you can do to manage the Configuration Manager console:

- **Modify the language that displays in the Configuration Manager console** - To modify the installed languages see Manage Configuration Manager console language in this topic.
- **Install additional consoles** - To install additional consoles, see Install System Center Configuration Manager consoles.
- **Configure DCOM** - To configure DCOM permission to enable consoles that are remote from the site server to connect, see Configure DCOM permissions for remote Configuration Manager consoles in this topic.
- **Modify permissions to limit what administrative users can see in the console** - To modify administrative permission, which limit what users can see and do in the console, see Modify the administrative scope of an administrative user.

Manage Configuration Manager console language

During site server installation, the Configuration Manager console installation files and supported language packs for the site are copied to the **<ConfigMgrInstallationPath>\Tools\ConsoleSetup** subfolder on the site server.

- When you start the Configuration Manager console installation from this folder on the site server, the Configuration Manager console and supported language pack files are copied to the computer
- When a language pack is available for the current language setting on the computer, the Configuration Manager console opens in that language
- If the associated language pack is not available for the Configuration Manager console, the console opens in English

For example, consider a scenario where you install the Configuration Manager console from a site server that supports English, German, and French. If you open the Configuration Manager console on a computer with a configured language setting of French, the console opens in French. If you open the Configuration Manager console on a computer with a configured language of Japanese, the console opens in English because the Japanese language pack is not available.

Each time the Configuration Manager console opens, it determines the configured language settings for the computer, verifies whether an associated language pack is available for the Configuration Manager console, and then opens the console by using the appropriate language pack. When you want to open the Configuration Manager console in English regardless of the configured language settings on the computer, you must manually remove or rename the language pack files on the computer.

Use the following procedures to start the Configuration Manager console in English regardless of the configured locale setting on the computer.

To install an English-only version of the Configuration Manager console on computers

1. In Windows Explorer, browse to **<ConfigMgrInstallationPath>\Tools\ConsoleSetup\LanguagePack**

2. Rename the **.msp** and **.mst** files. For example, you could change **<file name>.MSP** to **<file name>.MSP.disabled**.

3. Install the Configuration Manager console on the computer.

> **IMPORTANT**
> When new server languages are configured for the site server, the .msp and .mst files are recopied to the **LanguagePack** folder, and you must repeat this procedure to install new Configuration Manager consoles in only English.

To temporarily disable a console language on an existing Configuration Manager console installation

1. On the computer that is running the Configuration Manager console, close the Configuration Manager console.

2. In Windows Explorer, browse to <*ConsoleInstallationPath*>\Bin\ on the Configuration Manager console computer.

3. Rename the appropriate language folder for the language that is configured on the computer. For example, if the language settings for the computer were set for German, you could rename the **de** folder to **de.disabled**.

4. To open the Configuration Manager console in the language that is configured for the computer, rename the folder to the original name. For example, rename **de.disabled** to **de**.

Configure DCOM permissions for remote Configuration Manager consoles

The user account that runs the Configuration Manager console requires permission to access the site database by using the SMS Provider. However, an administrative user who uses a remote Configuration Manager console also requires **Remote Activation** DCOM permissions on:

- The site server computer
- Each computer that hosts an instance of the SMS Provider

The security group named **SMS Admins** grants access to the SMS Provider on a computer, and can also be used to grant the required DCOM permissions. (This group is local to the computer when the SMS Provider runs on a member server, and is a domain local group when the SMS Provider runs on a domain controller.)

> **IMPORTANT**
> The Configuration Manager console uses Windows Management Instrumentation (WMI) to connect to the SMS Provider, and WMI internally uses DCOM. Therefore, Configuration Manager requires permissions to activate a DCOM server on the SMS Provider computer if the Configuration Manager console is running on a computer other than the SMS Provider computer. By default, Remote Activation is granted only to the members of the built-in Administrators group. If you allow the SMS Admins group to have Remote Activation permission, a member of this group could attempt DCOM attacks against the SMS Provider computer. This configuration also increases the attack surface of the computer. To mitigate this threat, carefully monitor the membership of the SMS Admins group.

Use the following procedure to configure each central administration site, primary site server, and each computer where the SMS Provider is installed to grant remote Configuration Manager console access for administrative users.

To configure DCOM permissions for remote Configuration Manager console connections

1. Open **Component Services** by running **Dcomcnfg.exe**.

2. In **Component Services**, click **Console root** > **Component Services** > **Computers**, and then click **My Computer**. On the **Action** menu, click **Properties**.
3. In the **My Computer Properties** dialog box, on the **COM Security** tab, in the **Launch and Activation Permissions** section, click **Edit Limits**.
4. In the **Launch and Activation Permissions** dialog box, click **Add**.
5. In the **Select User, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select (examples)** box, type **SMS Admins**, and then click **OK**.

   > **NOTE**
   > You might have to change the setting for **From this Location** to locate the SMS Admins group. This group is local to the computer when the SMS Provider runs on a member server, and is a domain local group when the SMS Provider runs on a domain controller.

6. In the **Permissions for SMS Admins** section, to allow remote activation, select the **Remote Activation** check box.
7. Click **OK** and click **OK** again, and then close **Computer Management**. Your computer is now configured to allow remote Configuration Manager console access to members of the SMS Admins group.

   Repeat this procedure on each SMS Provider computer that might support remote Configuration Manager consoles.

Modify the site database configuration

After you install a site, you can modify the configuration of the site database and site database server by running Setup on a central administration site server or primary site server. You can move the site database to a new instance of SQL Server on the same computer, or to a different computer that runs a supported version of SQL Server. These and related changes are not supported for the database configuration at secondary sites.

For more information about the limits of support, see Support policy for manual database changes in a Configuration Manager environment.

> **NOTE**
> When you modify the database configuration for a site, Configuration Manager restarts or reinstalls Configuration Manager services on the site server and remote site system servers that communicate with the database.

To modify the database configuration, you must run Setup on the site server and select the option **Perform site maintenance or reset this site**. Next, select the **Modify SQL Server configuration** option. You can change the following site database configurations:

- The Windows-based server that hosts the database.
- The instance of SQL Server in use on a server that hosts the SQL Server database.
- The database name.
- SQL Server Port in use by Configuration Manager
- SQL Server Service Broker port in use by Configuration Manager

If you move the site database, you must configure the following:

- **Configure access:** When you move the site database to a new computer, add the computer account of the

site server to the **Local Administrators** group on the computer that runs SQL Server. If you use a SQL Server cluster for the site database, you must add the computer account to the **Local Administrators** group of each Windows Server cluster node computer.

- **Enable common language runtime (CLR) integration:** When you move the database to a new instance on SQL Server, or to a new SQL Server computer, you must enable common language runtime (CLR) integration. To enable CLR, use **SQL Server Management Studio** to connect to the instance of SQL Server that hosts the site database and run the following stored procedure as a query: **sp_configure 'clr enabled',1; reconfigure**.
- **Ensure the new SQL Server has access to the backup location:** When you use a UNC for storing your site database backup, after moving the database to a new server, including a move a SQL Server AlwaysOn availability group or to a SQL Server cluster, ensure the computer account of the new SQL Server has **write** permissions to the UNC location.

> **IMPORTANT**
>
> Before you move a database that has one or more database replicas for management points, you must first remove the database replicas. After you complete the database move, you can reconfigure database replicas. For more information see Database replicas for management points for System Center Configuration Manager.

Manage the SPN for the site database server

You can choose the account that runs SQL Services for the site database:

- When the services run with the computers system account, the SPN is automatically registered for you.
- When the services run with a domain local user account, you must manually register the SPN to ensure SQL clients and other site system can perform Kerberos authentication. Without Kerberos authentication, communication to the database might fail.

SQL Server documentation can help you manually register the SPN, and provide additional background about SPNs and Kerberos connections.

> **IMPORTANT**
>
> - When you create an SPN for a clustered SQL Server, you must specify the virtual name of the SQL Server Cluster as the SQL Server computer name
> - The command to register an SPN for a SQL Server named instance is the same as that you use when you register an SPN for a default instance except that the port number must match the port that is used by the named instance

You can register an SPN for the SQL Server service account of the site database server by using the **Setspn** tool. You must run the Setspn tool on a computer that resides in the domain of SQL Server, and it must use Domain Administrator credentials to run.

Use the following procedures as examples of how to manage the SPN for the SQL Server service account that uses the Setspn tool on Windows Server 2008 R2. For specific guidance about Setspn, see Setspn Overview, or similar documentation specific to your operating system.

> **NOTE**
>
> The following procedures reference the Setspn command-line tool. The Setspn command-line tool is included when you install Windows Server 2003 Support Tools from the product CD or from the Microsoft Download Center. For more information about how to install Windows Support Tools from the product CD, see Install Windows Support Tools.

To manually create a domain user Service Principal Name (SPN) for the SQL Server service account

1. On the **Start** menu, click **Run**, and then enter **cmd** in the Run dialog box.
2. At the command line, navigate to the Windows Server support tools installation directory. By default, these tools are located in the **C:\Program Files\Support Tools** directory.
3. Enter a valid command to create the SPN. To create the SPN, you can use the NetBIOS name or the fully qualified domain name (FQDN) of the computer running SQL Server. However, you must create an SPN for both the NetBIOS name and the FQDN.

   > **IMPORTANT**
   > When you create an SPN for a clustered SQL Server, you must specify the virtual name of the SQL Server Cluster as the SQL Server computer name.

   - To create an SPN for the NetBIOS name of the SQL Server computer, type the following command: **setspn -A MSSQLSvc/<SQL Server computer name>:1433 <Domain\Account>**
   - To create an SPN for the FQDN of the SQL Server computer, type the following command:**setspn -A MSSQLSvc/<SQL Server FQDN>:1433 <Domain\Account>**

   > **NOTE**
   > The command to register an SPN for a SQL Server named instance is the same as that you use when you register an SPN for a default instance except that the port number must match the port that is used by the named instance.

To verify the domain user SPN is registered correctly by using the Setspn command

1. On the **Start** menu, click **Run**, and then enter **cmd** in the **Run** dialog box.
2. At the command prompt, enter the following command: **setspn -L <domain\SQL Service Account>**.
3. Review the registered **ServicePrincipalName** to ensure that a valid SPN has been created for the SQL Server.

To verify the domain user SPN is registered correctly when using the ADSIEdit MMC console

1. On the **Start** menu, click **Run**, and then enter **adsiedit.msc** to start the ADSIEdit MMC console.
2. If necessary, connect to the domain of the site server.
3. In the console pane, expand the site server's domain, expand **DC=<server distinguished name>**, expand **CN=Users**, right-click **CN=<Service Account User>**, and then click **Properties**.
4. In the **CN=<Service Account User> Properties** dialog box, review the **servicePrincipalName** value to ensure that a valid SPN has been created and associated with the correct SQL Server computer.

To change the SQL Server service account from local system to a domain user account

1. Create or select a domain or local system user account that you want to use as the SQL Server service account.
2. Open **SQL Server Configuration Manager**.
3. Click **SQL Server Services**, and then double-click **SQL Server<INSTANCE NAME>**.
4. On the **Log on** tab, select **This account**, and then enter the user name and password for the domain user account created in step 1, or click **Browse** to find the user account in Active Directory Domain Services, and then click **Apply**.
5. Click **Yes** in the **Confirm Account Change** dialog box to confirm the service account change and restart

the SQL Server Service.

6. Click **OK** after the service account has been successfully changed.

Run a site reset

When a site reset runs at a central administration site or primary site, the site:

- Reapplies the default Configuration Manager file and registry permissions
- Reinstalls all site components and all site system roles at the site

Secondary sites do not support a site reset.

Site resets can be run manually, when you choose, but can also run automatically after you modify the site configuration.

For example, if there has been a change to the accounts used by Configuration Manager components, you should consider a manual site reset to ensure the site components update to use the new account details. However, if you modify the client or server languages at a site, Configuration Manager automatically runs a site reset because the reset is required before a site can use this change.

> **NOTE**
> A site reset does not reset access permissions to non-Configuration Manager objects.

When a site reset runs:

1. Setup stops and restarts the **SMS_SITE_COMPONENT_MANAGER** service and the thread components of the **SMS_EXECUTIVE** service.
2. Setup removes, and then re-creates, the site system share folder and the **SMS Executive** component on the local computer and on remote site system computers.
3. Setup restarts the **SMS_SITE_COMPONENT_MANAGER** service, this service installs the **SMS_EXECUTIVE** and the **SMS_SQL_MONITOR** services.

In addition, a site reset restores the following objects:

- The **SMS** or **NAL** registry keys, and any default subkeys under these keys.
- The Configuration Manager file directory tree, and any default files or subdirectories in this file directory tree.

Prerequisites to run a site reset

The account that you use to perform a site reset must have the following permissions:

- The account that you use to perform a site reset must have the following permissions:
  - **Central administration site**: The account that you use to run a site reset at this site must be a local administrator on the central administration site server and must have privileges that are equivalent to the **Full Administrator** role-based administration security role.
  - **Primary site**: The account that you use to run a site reset at this site must be a local administrator on the primary site server and must have privileges that are equivalent to the **Full Administrator** role-based administration security role. If the primary site is in a hierarchy with a central administration site, this account must also be a local administrator on the central administration site server.

Limitations for a site reset

- Beginning with version 1602, you cannot use a site reset to change the Server or Client language packs that installed at sites so long as the hierarchy is configured to support testing client upgrades in a pre-production collection.

To perform a site reset

1. Run **Configuration Manager Setup** from **<Configuration Manager site installation folder>\BIN\X64\setup.exe**.

   > **TIP**
   > You can also run a site reset by starting Configuration Manager Setup on the **Start** menu of the site server computer or from the Configuration Manager source media.

2. On the **Getting Started** page, select **Perform site maintenance or reset this site**, and then click **Next**.
3. On the **Site Maintenance** page, select **Reset site with no configuration changes**, and then click **Next**.
4. Click **Yes** to begin the site reset.

When the site reset is finished, click **Close** to complete this procedure.

Manage language packs at a site

After a site installs, you can change the server and client language packs that are in use:

Server language packs:

- **Applies to:**

  Configuration Manager console installations

  New installations of applicable site system roles

- **Details:**

  After you update the server language packs at a site, you can add support for the language packs to Configuration Manager consoles.

  To add support for a server language pack to a Configuration Manager console, you must install the Configuration Manager console from the **ConsoleSetup** folder on a site server that includes the language pack that you want to use. If the Configuration Manager console is already installed, you must first uninstall it to enable the new installation to identify the current list of supported language packs.

Client language packs:

- **Applies to:**

  Changes to the client language packs update the client installation source files so that new client installations and upgrades add support for the updated list of client languages.

- **Details:**

  After you update the client language packs at a site, you must install each client that will use the language packs by using source files that include the client language packs.

For information about the client and server languages that are supported by Configuration Manager, see Language Packs in System Center Configuration Manager

To modify the language packs that are supported at a site

1. On the site server, run Configuration Manager Setup from **<Configuration Manager site installation**

folder>\BIN\X64\setup.exe.

2. On the **Getting Started** page, select **Perform site maintenance or reset this Site**, and then click **Next**.
3. On the **Site Maintenance** page, select **Modify language configuration**, and then click **Next**.
4. On the **Prerequisites Downloads** page, select **Download required files** to acquire updates to language packs, or select **Use previously downloaded files** to use previously downloaded files that include the language packs you want to add to the site. Click **Next** to validate the files and continue.
5. On the **Server Language Selection** page, select the check box for server languages this site supports, and then click **Next**.
6. On the **Client Language Selection** page, select the check box for client languages that this site supports, and then click **Next**.
7. Click **Next**, to modify language support at the site.

   > **NOTE**
   > Configuration Manager initiates a site reset which also reinstalls all site system roles at the site.

8. Click **Close** to complete this procedure.

Modify the database server alert threshold

By default, Configuration Manager generates alerts when free disk space on a site database server is low. The defaults are set to generate a warning when there is 10 GB or less of free disk space, and a critical alert when there is 5 GB or less of free disk space. You can modify these values or disable alerts for each site.

To change these settings:

1. In the **Administration** workspace, expand **Site Configuration**, and then click **Sites**.
2. Select the site that you want to configure and open that site's **Properties**.
3. In the site's **Properties** dialog box, select the **Alert** tab, and then edit the settings.
4. Click **OK** to close the site properties dialog box.

The CD.Latest folder for Configuration Manager

5/9/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager has a process to deliver updates to the product from within the Configuration Manager console. To support this new method of updating Configuration Manager, a new folder is created named **CD.Latest**. This folder contains a copy of the Configuration Manager installation files for the updated version of your site.

The CD.Latest folder contains a folder named **Redist**, which contains the redistributable files that setup downloads and uses. These files are matched to the version of Configuration Manager files found in that CD.Latest folder. When you run Setup from a CD.Latest folder, you must use files that are matched to that version of Setup. You can either direct Setup to download new and current files from Microsoft, or direct Setup to use the files from the Redist folder included in the CD.Latest folder.

Baseline media doesn't include a **Redist** folder. The site doesn't create a Redist folder until you install an in-console update. In the meantime, use the Redist folder that you used when installing sites from the baseline media.

> **TIP**
> Make sure the redistributable files you use are current. If you haven't recently downloaded redistributable files, plan to allow Setup to do so from Microsoft.

The following scenarios create or update the CD.Latest folder on a central administration site or primary site server:

- When you install an update or hotfix from within the Configuration Manager console, the site creates or updates the folder in the Configuration Manager installation folder.
- When you run the built-in Configuration Manager backup task, the site creates or updates the folder under the designated backup folder location.
- When you install a new site using baseline media, the site creates the CD.Latest folder.

Supported scenarios

The source files from the CD.Latest folder are supported for the following scenarios:

Backup and recovery

To recover a site, use the source files from a CD.Latest folder that matches your site. When you run a site backup using the built-in site backup task, the CD.Latest folder is included as part of the backup.

- When you reinstall a site as part of a site recovery, you install the site from the CD.Latest folder included in your backup. This action installs the site using the file versions that match your site backup and site database.
  - If you don't have access the correct CD.Latest folder version, get the CD.Latest folder with the correct file versions by installing a site in a lab environment. Then update that site to match the version you want to recover.
  - If you don't have the correct CD.Latest folder and its contents available, you can't recover a site. In

this circumstance, you need to reinstall the site.

- When you don't have a CD.Latest folder, but do have a working child primary site or central administration site, you can use that site as a reference site for a site recovery.

Install a child primary site

When you want to install a new child primary site below a central administration site that has installed one or more in-console updates, use Setup and the source files from the CD.Latest folder from the central administration site. This process uses installation source files that match the version of the central administration site. For more information, see Use the Setup Wizard to install sites.

Expand a stand-alone primary site

When you expand a stand-alone primary site by installing a new central administration site, use Setup and the source files from the CD.Latest folder from the primary site. This process uses installation source files that match the version of the primary site. For more information, see Expand a stand-alone primary site.

Install a secondary site

When you want to install a new secondary site below a primary site that has installed one or more in-console updates, use the source files from the CD.Latest folder from the primary site.

For more information, see Install a secondary site.

Unsupported scenarios

The updated CD.Latest source files aren't supported for:

- Installing a new site for a new hierarchy
- Upgrading a Microsoft System Center 2012 Configuration Manager site to System Center Configuration Manager, current branch
- Installing Configuration Manager clients
- Installing Configuration Manager consoles

Upgrade on-premises infrastructure that supports Configuration Manager

9/5/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the information in this article to help you upgrade the server infrastructure that runs Configuration Manager.

- If you want to *upgrade* from an earlier version to Configuration Manager, current branch, see Upgrade to Configuration Manager.
- If you want to *update* your Configuration Manager, current branch, infrastructure to a new version, see Updates for Configuration Manager.

Upgrade the OS of site systems

Configuration Manager supports the in-place upgrade of the server OS that hosts a site server and any site system role, in the following situations:

- If Configuration Manager still supports the resulting service pack level of Windows, it supports in-place upgrade to a later Windows Server service pack.
- In-place upgrade from:
  - Windows Server 2016 to Windows Server 2019
  - Windows Server 2012 R2 to Windows Server 2019
  - Windows Server 2012 R2 to Windows Server 2016
  - Windows Server 2012 to Windows Server 2016
  - Windows Server 2012 to Windows Server 2012 R2
  - Windows Server 2008 R2 to Windows Server 2012 R2

To upgrade a server, use the upgrade procedures provided by the OS you're upgrading to. See the following articles:

- Windows Server Upgrade Center
- Upgrade and conversion options for Windows Server 2016
- Upgrade Options for Windows Server 2012 R2

Upgrade to Windows Server 2016 or 2019

Use the steps in this section for any of the following upgrade scenarios:

- Upgrade either Windows Server 2012 R2 or Windows Server 2016 to Windows Server 2019
- Upgrade either Windows Server 2012 or Windows Server 2012 R2 to Windows Server 2016

Before upgrade

- (Windows Server 2012 or Windows Server 2012 R2): Remove the System Center Endpoint Protection (SCEP) client. Windows Server now has Windows Defender built in, which replaces the SCEP client. The presence of the SCEP client can prevent an upgrade to Windows Server.

- Remove the WSUS role from the server if it's installed. You may keep the SUSDB and reattach it once WSUS is reinstalled.
- If you're upgrading the OS of the site server, make sure file-based replication is healthy for the site. Check all inboxes for a backlog on both sending and receiving sites. If there are lots of stuck or pending replication jobs, wait until they clear out.
  - On the sending site, review **sender.log**.
  - On the receiving site, review **despooler log**.

After upgrade

- Make sure Windows Defender is enabled, set for automatic start, and running.
- Make sure the following Configuration Manager services are running:
  - SMS_EXECUTIVE
  - SMS_SITE_COMPONENT_MANAGER
- Make sure the **Windows Process Activation** and **WWW/W3svc** services are enabled and set for automatic start. The upgrade process disables these services, so make sure they're running for the following site system roles:
  - Site server
  - Management point
  - Application Catalog web service point
  - Application Catalog website point
- Make sure each server that hosts a site system role continues to meet all prerequisites. For example, you might need to reinstall BITS, WSUS, or configure specific settings for IIS.
- After restoring any missing prerequisites, restart the server one more time to make sure services are started and operational.
- If you're upgrading the primary site server, then run a site reset.

Known issue for remote Configuration Manager consoles

After you upgrade the site server, or an instance of the SMS Provider, you can't connect with the Configuration Manager console. To work around this problem, manually restore permissions for the **SMS Admins** group in WMI. Permissions must be set on the site server, and on each remote server that hosts an instance of the SMS Provider:

1. On the applicable servers, open the Microsoft Management Console (MMC) and add the snap-in for **WMI Control**, and then select **Local computer**.
2. In the MMC, open the **Properties** of **WMI Control (Local)** and select the **Security** tab.
3. Expand the tree below Root, select the **SMS** node, and then choose **Security**. Make sure the **SMS Admins** group has the following permissions:
   - Enable Account
   - Remote Enable
4. On the **Security tab** below the **SMS** node, select the **site_<sitecode>** node, and then choose **Security**. Make sure the **SMS Admins** group has the following permissions:
   - Execute Methods

- Provider Write
- Enable Account
- Remote Enable

5. Save the permissions to restore access for the Configuration Manager console.

Known issue for remote site systems

After you upgrade a server that hosts a site system role, the value `Software\Microsoft\SMS` may be missing from the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths`

If this value is missing after you upgrade Windows on the server, manually add it. Otherwise site system roles can have issues uploading files to the site server inboxes.

Upgrade to Windows Server 2012 R2

When you upgrade from either Windows Server 2008 R2 or Windows Server 2012 to Windows Server 2012 R2, the following conditions apply:

Before upgrade

- On Windows Server 2012: Remove the WSUS role from the server if it's installed. You may keep the SUSDB and reattach it once WSUS is reinstalled.
- On Windows Server 2008 R2: Before you upgrade to Windows Server 2012 R2, you must uninstall WSUS 3.2 from the server. You may keep the SUSDB and reattach it once WSUS is reinstalled. For more information, see Windows Server Update Services Overview.
- If you're upgrading the OS of the site server, make surefile-based replication is healthy for the site. Check all inboxes for a backlog on both sending and receiving sites. If there are lots of stuck or pending replication jobs, wait until they clear out.
  - On the sending site, review **sender.log**.
  - On the receiving site, review **despooler log**.

After upgrade

- The upgrade process disables the Windows Deployment Services. Make sure this service is started and running for the following site system roles:
  - Site server
  - Management point
  - Application Catalog web service point
  - Application Catalog website point
- Make sure the **Windows Process Activation** and **WWW/W3svc** services are enabled and set for automatic start. The upgrade process disables these services, so make sure they're running for the following site system roles:
  - Site server
  - Management point
  - Application Catalog web service point
  - Application Catalog website point
- Make sure each server that hosts a site system role continues to meet all prerequisites. For example, you might need to reinstall BITS, WSUS, or configure specific settings for IIS.

After restoring any missing prerequisites, restart the server one more time to make sure services are started and operational.

Unsupported upgrade scenarios

The following Windows Server upgrade scenarios are commonly asked about, but not supported by Configuration Manager:

- Windows Server 2008 to Windows Server 2012 or later
- Windows Server 2008 R2 to Windows Server 2012

Upgrade the OS of clients

Configuration Manager supports an in-place upgrade of the OS for Configuration Manager clients in the following situations:

- If Configuration Manager supports the resulting service pack level, it supports in-place upgrade to a later Windows service pack.
- In-place upgrade of Windows from a supported version to Windows 10. For more information, see Upgrade Windows to the latest version.
- Build-to-build servicing upgrades of Windows 10. For more information, see Manage Windows as a service.

Upgrade SQL Server

Configuration Manager supports an in-place upgrade of SQL Server on the site database server.

For information about the versions of SQL Server that Configuration Manager supports, see Support for SQL Server versions.

Upgrade the service pack version of SQL Server

If Configuration Manager still supports the resulting SQL Server service pack level, it supports the in-place upgrade of SQL Server to a later service pack.

When you have more than one Configuration Manager site in a hierarchy, each site can run a different service pack version of SQL Server. There's no limitation to the order in which sites upgrade the service pack version of SQL Server.

Upgrade to a new version of SQL Server

Configuration Manager supports the in-place upgrade of SQL Server to the following versions:

- SQL Server 2017
- SQL Server 2016
- SQL Server 2014

This includes the upgrade of SQL Server Express to a newer version of SQL Server Express at secondary sites.

When you upgrade the version of SQL Server that hosts the site database, you must upgrade the SQL Server version that's used at sites in the following order:

1. Upgrade SQL Server at the central administration site first
2. Upgrade secondary sites before you upgrade a secondary site's parent primary site
3. Upgrade parent primary sites last. These sites include both child primary sites that report to a central administration site, and stand-alone primary sites that are the top-level site of a hierarchy.

SQL Server cardinality estimation level

When you upgrade a site database from an earlier version of SQL Server, the database keeps its existing SQL cardinality estimation level, if it's at the minimum allowed for that instance of SQL Server. Upgrading SQL Server with a database at a compatibility level lower than the allowed level automatically sets the database to the lowest compatibility level allowed by SQL Server.

The following table identifies the recommended compatibility levels for Configuration Manager site databases:

SQL SERVER VERSION	SUPPORTED COMPATIBILITY LEVELS	RECOMMENDED LEVEL
SQL Server 2017	140, 130, 120, 110	140
SQL Server 2016	130, 120, 110	130
SQL Server 2014	120, 110	110

To identify the SQL Server cardinality estimation compatibility level in use for your site database, run the following SQL query on the site database server:

```
SELECT name, compatibility_level FROM sys.databases
```

For more information on SQL CE compatibility levels and how to set them, see ALTER DATABASE Compatibility Level (Transact-SQL).

For more information about upgrading SQL Server, see the following SQL Server articles:

- Upgrade to SQL Server 2017
- Upgrade to SQL Server 2016
- Upgrade to SQL Server 2014

To upgrade SQL Server on the site database server

1. Stop all Configuration Manager services at the site
2. Upgrade SQL Server to a supported version
3. Restart the Configuration Manager services

> **NOTE**
> When you change the SQL Server edition in use at the central administration site from Standard to either a Datacenter or Enterprise, the database partition doesn't change. This database partition limits the number of clients the hierarchy supports.

Updates and servicing for Configuration Manager

7/29/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager uses an in-console service method called **Updates and Servicing**. This in-console method makes it easy to find and install recommended updates for your Configuration Manager infrastructure. In-console servicing is supplemented by out-of-band updates such as hotfixes. The out-of-band updates are intended for customers who need to resolve issues that might be specific to their environment.

> **TIP**
> The terms *upgrade*, *update*, and *install* are used to describe three separate concepts in Configuration Manager. For more information about how each term is used, see About upgrade, update, and install.

Baseline and update versions

Use the latest baseline version when you install a new site in a new hierarchy.

- Also use a baseline version to upgrade from System Center 2012 Configuration Manager.
- After upgrading to Configuration Manager current branch, don't use baseline versions to stay current. Instead, only use in-console updates to update to the newest version.
- Periodically, additional baseline versions are released. When you use the latest baseline version to install a new hierarchy, you avoid installing an outdated or unsupported version of Configuration Manager, followed by an additional upgrade of your infrastructure to bring it up-to-date.

After you install a baseline version, additional versions of Configuration Manager are available as in-console updates. In-console updates update your infrastructure to the latest version of Configuration Manager.

- You install in-console updates to update the version of your top-level site.
- Updates you install at the central administration site automatically install at child primary sites. Control this timing by using a maintenance window at the primary site.
- Manually update secondary sites to a new update version from within the console.

When you install an update, the update stores installation files for that version on the site server in a folder named **CD.Latest**. For more information about these files, see The CD.Latest folder.

- Use the files in the CD.Latest folder during site recovery. Also, when your hierarchy no longer runs a baseline version, use these files to install additional sites.
- You can't use installation files from CD.Latest to install the first site of a new hierarchy, or to upgrade a site from System Center 2012 Configuration Manager.

Version details

Some updates for Configuration Manager are available as both an in-console update version for existing infrastructure, and as a new baseline version.

Supported versions

The following supported versions of Configuration Manager are currently available as a baseline, an update, or both:

VERSION	AVAILABILITY DATE	SUPPORT END DATE	BASELINE	IN-CONSOLE UPDATE
1906 5.00.8853.1000	July 26, 2019	January 26, 2021	No	Yes
1902 5.00.8790.1000	March 27, 2019	September 27, 2020	Yes[Note 1]	Yes
1810 5.00.8740.1000	November 27, 2018	May 27, 2020	No	Yes
1806 5.00.8692.1000	July 31, 2018	January 31, 2020	No	Yes
1802 5.00.8634.1000	March 22, 2018	September 22, 2019	Yes[Note 1]	Yes

NOTE

Note 1: The baseline media is available as part of the following releases on the Volume License Service Center (VLSC):

- System Center Config Mgr (current branch)
- System Center 2016 Datacenter
- System Center 2016 Standard

For example, search the VLSC for `System Center Config Mgr (current branch)`. Find the baseline media in the list of files, and download for that release.

Historical versions

The following table lists historical versions of Configuration Manager current branch that are out of support:

VERSION	AVAILABILITY DATE	SUPPORT END DATE	BASELINE	IN-CONSOLE UPDATE
1710 5.00.8577.1000	November 20, 2017	May 20, 2019	No	Yes
1706 5.00.8540.1000	July 31, 2017	July 31, 2018	No	Yes
1702 5.00.8498.1000	March 27, 2017	March 27, 2018	Yes	Yes
1610 5.00.8458.1000	November 18, 2016	November 18, 2017	No	Yes

VERSION	AVAILABILITY DATE	SUPPORT END DATE	BASELINE	IN-CONSOLE UPDATE
1606 5.00.8412.1000	July 22, 2016	July 22, 2017	No	Yes
1606 with the 1606 hotfix rollup (KB3186654) 5.00.8412.1307	October 12, 2016	October 12, 2017	Yes	No
1602 5.00.8355.1000	March 11, 2016	March 11, 2017	No	Yes
1511 5.00.8325.1000	December 8, 2015	December 8, 2016	Yes	No

How to check the version

To check the version of your Configuration Manager site, in the console go to **About System Center Configuration Manager** at the top-left corner of the console. This dialog displays the site and console versions.

> **NOTE**
> The console version is slightly different from the site version. The minor version of the console corresponds to the Configuration Manager release version. For example, in Configuration Manager version 1802 the initial site version is 5.0.8634.1000, and the initial console version is 5.**1802**.1082.1700. The build (1082) and revision (1700) numbers may change with future hotfixes.

In-console updates and servicing

When you use a production-ready installation of Configuration Manager current branch, most updates are available using the **Updates and Servicing** channel. This method identifies, downloads, and makes available the updates that apply to your current infrastructure version and configuration. It includes only updates that Microsoft recommends for all customers.

These updates include:

- New versions, like version 1806, 1810, or 1902.
- Updates that include new features for your current version.
- Hotfixes for your version of Configuration Manager and that all customers should install.

> **NOTE**
> Starting in version 1902, in-console hotfixes now have supersedence relationships. For more information, see Supersedence for in-console hotfixes.

The in-console updates deliver increased stability and resolve common issues. They replace the update types seen for previous product versions such as service packs, cumulative updates, hotfixes that are applicable to all customers, and the extension for Microsoft Intune.

The in-console updates can apply to one or more of the following systems:

- Primary and central administration site servers
- Site system roles and site system servers
- Instances of the SMS Provider
- Configuration Manager consoles
- Configuration Manager clients

Configuration Manager discovers new updates for you. Synchronize your Configuration Manager service connection point with the Microsoft cloud service, noting the following behaviors:

- When your service connection point is in online mode, your site synchronizes with Microsoft every day. It automatically identifies new updates that apply to your infrastructure. To download updates and redistributable files, the computer that hosts the service connection point site system role uses the **System** context to access the following internet locations: go.microsoft.com and download.microsoft.com. For more information about additional locations used by the service connection point, see Internet access requirements.
- When your service connection point is in offline mode, use the service connection tool to manually sync with the Microsoft cloud. For more information, see Use the service connection tool.
- In-console updates replace the need to independently locate and install individual updates, service packs, and new features.
- Install only the in-console updates you choose. When installing some updates, you can select individual features to enable and use. For more information, see Enable optional features from updates.

When you install an in-console update, the following process occurs:

- It automatically runs a prerequisite check. You can also manually run this check prior to starting the installation.
- It installs at the top-level site in your environment. This site is the central administration site if you have one. In a hierarchy, the update automatically installs at primary sites. Control when each primary site server is allowed to update by using Service windows for site servers.
- After a site server updates, all affected site system roles automatically update. These roles include instances of the SMS Provider. After the site installs the update, Configuration Manager consoles also prompt the console user to update the console.
- If an update includes the Configuration Manager client, you're offered the option to test the update in pre-production, or to apply the update to all clients immediately.
- After a primary site is updated, secondary sites don't automatically update. Instead, you must manually initiate the secondary site update.

> **NOTE**
> The Configuration Manager current branch, the long-term servicing branch, and the technical preview branch are different releases. Updates that apply for one branch aren't available as in-console updates for the other branches. For more information about available branches, see Which branch of Configuration Manager should I use?.

Supersedence for in-console hotfixes

Starting in version 1902, in-console hotfixes now have supersedence relationships. When Microsoft publishes a new Configuration Manager hotfix, the console doesn't display any hotfixes that are superseded by this new hotfix. This new behavior helps you better determine which hotfixes to install.

Supersedence example

There are three hotfixes available: Hotfix-A, Hotfix-B, and Hotfix-C. Hotfix-A is superseded by Hotfix-B, and Hotfix-B is superseded by Hotfix-C.

HOTFIX-A	HOTFIX-B	HOTFIX-C	IN-CONSOLE VIEW
Not installed	Not installed	Not installed	Show all three hotfixes
Installed	Installed	Not installed	Hotfix-B shows as installed Hotfix-C shows as ready to install
Not installed	Not installed	Installed	Hotfix-C shows as installed

Out-of-band hotfixes

Some hotfixes release with limited availability to address specific issues. Other hotfixes are applicable to all customers but can't install using the in-console method. These fixes are delivered out-of-band and not discovered from the Microsoft cloud service.

Typically, when you're seeking to fix or address a problem with your deployment of Configuration Manager, you can learn about out-of-band hotfixes from Microsoft customer support services, a Microsoft support knowledge base article, or the Configuration Manager team blog.

Install these fixes manually, using one of the following two methods:

Update Registration Tool

This tool manually imports the hotfix into your Configuration Manager console. Then install the update as you would in-console updates that are discovered automatically.

This method is used for hotfixes that use the following file name structure:

```
<Product>-<product version>-<KB article ID>-ConfigMgr.Update.exe
```

For more information, see Use the update registration tool to import hotfixes.

Hotfix Installer

Use this tool to manually install a hotfix that can't be installed using the in-console method.

This method is used for fixes that use the following file name structure:

```
<Product>-<product version>-<KB article ID>-<platform>-<language>.exe
```

For more information, see Use the hotfix installer to install updates.

Next steps

The following articles can help you understand how to find and install the different update types for Configuration Manager:

- Install in-console updates
- Use the service connection tool
- Use the update registration tool to import hotfixes
- Use the hotfix installer to install updates

For more information about the technical preview branch, see Technical preview.

Install in-console updates for Configuration Manager

8/28/2019 • 18 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager synchronizes with the Microsoft cloud service to get updates. Then install these updates from within the Configuration Manager console.

Get available updates

The site only downloads updates that apply to your infrastructure and version. This synchronization can be automatic or manual, depending on how you configure the service connection point for your hierarchy:

- In **online mode**, the service connection point automatically connects to the Microsoft cloud service and downloads applicable updates.

  By default, Configuration Manager checks for new updates every 24 hours. Manually check for updates in the Configuration Manager console. Go to the **Administration** workspace, select the **Updates and Servicing** node, and choose **Check for Updates** in the ribbon.

- In **offline mode**, the service connection point doesn't connect to the Microsoft cloud service. To download and then import available updates, use the Service Connection Tool.

> **NOTE**
> If necessary, import out-of-band fixes into your console. To do so, use the update registration tool. These out-of-band fixes supplement the updates you get when you synchronize with the Microsoft cloud service.

After updates synchronize, view them in the Configuration Manager console. Go to the **Administration** workspace and select the **Updates and Servicing** node.

- Updates you haven't installed display as **Available**.
- Updates you've installed display as **Installed**. Only the most recently installed update is shown. To view previously installed updates, select **History** in the ribbon.

Before you configure the service connection point, understand and plan for its additional uses. The following uses might affect how you configure this site system role:

- The site uses the service connection point to upload usage information about your site. This information helps the Microsoft cloud service identify the updates that are available for the current version of your infrastructure. For more information, see Diagnostics and usage data.
- The site uses the service connection point to manage devices with Microsoft Intune, and using Configuration Manager on-premises mobile device management. For more information, see Hybrid mobile device management (MDM).

To better understand what happens when updates are downloaded, see the following flowcharts:

- Flowchart - Download updates
- Flowchart - Update replication

Assign permissions to view and manage updates and features

To view updates in the console, a user must have a role-based administration security role that includes the security class **Update packages**. This class grants access to view and manage updates in the Configuration Manager console.

About the Update packages class

By default, the **Update packages** class (SMS_CM_Updatepackages) is part of the following built-in security roles with the listed permissions:

- **Full Administrator** with **Modify** and **Read** permissions:
  - A user with this security role and access to the **All** security scope can view and install updates. The user can also enable features during the installation, and enable individual features after the site updates.
  - A user with this security role and access to the **Default** security scope can view and install updates. The user can also enable features during the installation, and view features after the site updates. But this user can't enable the features after the site updates.
- **Read-only Analyst** with **Read** permissions:
  - A user with this security role and access to the **Default** scope can view updates but not install them. This user can also view features after the site updates, but can't enable them.

Permissions required for updates and servicing

- Use an account to which you assign a security role that includes the **Update packages** class with both **Modify** and **Read** permissions.
- Assign the account to the **Default** scope.

Permissions to only view updates

- Use an account to which you assign a security role that includes the **Update packages** class with only the **Read** permission.
- Assign the account to the **Default** scope.

Permissions required to enable features after the site updates

- Use an account to which you assign a security role that includes the **Update packages** class with both **Modify** and **Read** permissions.
- Assign the account to the **All** scope.

Before you install an in-console update

Review the following steps before you install an update from within the Configuration Manager console.

Step 1: Review the update checklist

Review the applicable update checklist for actions to take before you start the update:

- Checklist for installing update 1906
- Checklist for installing update 1902
- Checklist for installing update 1810
- Checklist for installing update 1806

Step 2: Run the prerequisite checker before installing an update

Before you install an update, consider running the prerequisite check for that update. If you run the prerequisite before installing an update:

- The site replicates update files to other sites before installing the update.
- When you choose to install the update, the prerequisite check automatically runs again.

> **NOTE**
>
> When you start a prerequisite check and then view the status, the **Installation** phase appears to be active. However, the site isn't actually installing the update. To run the prerequisite check, the update process extracts the package from the content library. It then puts the package into a staging folder where it can access the current prerequisite checks. When you install an update, this same process runs. This behavior is why the Installation phase shows as **In progress**. Only the *Extract Update package* step is shown in the Installation category.

Later, when you install the update, you can configure the update to ignore prerequisite check warnings.

To run the prerequisite checker before installing an update

1. In the Configuration Manager console, go to the **Administration** workspace, and select the **Updates and Servicing** node.
2. Select the update package for which you want to run the prerequisite check.
3. Select **Run prerequisite check** in the ribbon.

   When you run the prerequisite check, content for the update replicates to child sites. View the **distmgr.log** on the site server to confirm that content replicates successfully.
4. To view the results of the prerequisite check:

   a. In the Configuration Manager console, go to the **Monitoring** workspace.

   b. Select the **Updates and Servicing Status** node and look for the prerequisite status.

   c. For more information, see the **ConfigMgrPrereq.log** on the site server.

Install in-console updates

When you're ready to install updates from within the Configuration Manager console, begin with the top-level site of your hierarchy. This site is either the central administration site or a standalone primary site.

Install the update outside of normal business hours for each site to minimize the effect on business operations. The update installation might include actions like reinstalling site components and site system roles.

- Child primary sites automatically start the update after the central administration site completes installation of the update. This process is by default and recommended. To control when a primary site installs updates, use Service windows for site servers.
- After the primary parent site update is complete, manually update secondary sites from within the Configuration Manager console. Automatic update of secondary site servers isn't supported.
- When you use a Configuration Manager console after the site is updated, you're prompted to update the console.
- After the site server successfully completes installation of an update, it automatically updates all applicable site system roles. However, all distribution points don't reinstall and go offline to update at the same time. Instead, the site server uses the site's content distribution settings to distribute the update to a subset of distribution points at a time. The result is that only some distribution points go offline to install the update. Distribution points that haven't begun to update or that have completed the update remain online and able

to provide content to clients.

Overview of in-console update installation

1. When the update installation starts

You're presented with the Updates Wizard that displays a list of the product areas that the update applies to.

- On the **General** page of the wizard, configure **Prerequisite warnings** as necessary:
  - Prerequisite errors always stop the update installation. Fix errors before you can successfully retry the update installation. For more information, see Retry installation of a failed update.
  - Prerequisite warnings can also stop the update installation. Fix warnings before you retry the update installation. For more information, see Retry installation of a failed update.
  - **Ignore any prerequisite check warnings and install this update regardless of missing requirements**: Set a condition for the update installation to ignore prerequisite warnings. This option allows the update installation to continue. If you don't select this option, the update installation stops when the process encounters a warning. Unless you've previously run the prerequisite check and fixed prerequisite warnings for a site, don't use this option.

    In both the **Administration** and **Monitoring** workspaces, the Updates and Servicing node includes a button on the ribbon named **Ignore prerequisite warnings**. This button becomes available when an update package fails to complete installation due to prerequisite check warnings. For example, you install an update without using the option to ignore prerequisite warnings (from within the Updates Wizard). The update installation stops with a state of prerequisite warning but no errors. Later, you select **Ignore prerequisite warnings** in the ribbon. This action triggers an automatic continuation of that update installation, which ignores prerequisite warnings. When you use this option, the update installation automatically continues after a few minutes.
- When an update applies to the Configuration Manager client, choose to test the client update with a limited set of clients. For more information, see How to test client upgrades in a pre-production collection.

2. During the update installation

As part of the update installation, Configuration Manager does the following actions:

- Reinstalls any affected components, like site system roles or the Configuration Manager console.
- Manages updates to clients based on the selections that you made for client piloting, and for automatic client upgrades.
- Site system servers generally don't need to restart as part of the update. If a role uses .NET, and the package updates that prerequisite component, then the site system may restart.

> **TIP**
> When you install Configuration Manager updates, the site also updates the CD.Latest folder. For more information, see The CD.Latest folder.

3. Monitor the progress of updates as they install

Use the following steps to monitor progress:

- In the Configuration Manager console, go to the **Administration** workspace, and select the **Updates and Servicing** node. This node shows the installation status for all update packages.
- In the Configuration Manager console, go to the **Monitoring** workspace, and select the **Updates and Servicing Status** node. This node shows the installation status of only the current update package that the site is installing.

The update installation is divided into several phases for easier monitoring. For each of the following phases, additional details in the installation status include which log file to view for more information:

  - **Download**: This phase applies only to the top-level site with the service connection point.
  - **Replication**
  - **Prerequisites Check**
  - **Installation**
  - **Post Installation**: For more information, see post installation tasks.

- View the **CMUpdate.log** file in `<ConfigMgr_Installation_Directory>\Logs` on the site server.

> **NOTE**
> - Starting in version 1906, you can see the state of the **Upgrade ConfigMgr database** task during the **Installation** phase.
>   - If the database upgrade is blocked, then you'll be given the warning **In progress, needs attention**.
>   - The cmupdate.log will log the program name and sessionid from SQL that is blocking the database upgrade.
>   - When the database upgrade is no longer blocked, the status will be reset to **In progress** or **Complete**.
>   - When the database upgrade is blocked, a check is done every 5 minutes to see if it's still blocked.

4. When the update installation completes

After the first site update completes installation:

- Child primary sites install the update automatically. No further action is required.
- Manually update secondary sites from within the Configuration Manager console. For more information, see start the update installation at a secondary site.
- Until all sites in your hierarchy update to the new version, your hierarchy operates in a mixed version mode. For more information, see Interoperability between different versions.

5. Update Configuration Manager consoles

After a central administration site or primary site updates, each Configuration Manager console that connects to the site must also update. You're prompted to update a console:

- When you open the console
- When you go to a new node in an open console

Update the console right away after the site updates.

After the console update completes, verify the console and site versions are correct. Go to **About System Center Configuration Manager** at the top-left corner of the console.

> **NOTE**
> The console version is slightly different from the site version. The minor version of the console corresponds to the Configuration Manager release version. For example, in Configuration Manager version 1802 the initial site version is 5.0.8634.1000, and the initial console version is 5.**1802**.1082.1700. The build (1082) and revision (1700) numbers may change with future hotfixes.

To start the update installation at the top-level site

At the top-level site of your hierarchy, in the Configuration Manager console, go to the **Administration** workspace, and select the **Updates and Servicing** node. Select an update with the state of **Available**, and then

choose **Install Update Pack** in the ribbon.

To start the update installation at a secondary site

After a secondary site's parent primary site updates, update the secondary site from within the Configuration Manager console. To do so, you use the **Upgrade Secondary Site Wizard**.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node. Select the secondary site you want to update, and then choose **Upgrade** in the ribbon.

2. Select **Yes** to start the update of the secondary site.

To monitor the update installation on a secondary site, select the secondary site, and choose **Show Install Status** in the ribbon. Also add the **Version** column to the Sites node so that you can view the version of each secondary site.

In some instances, the status in the console doesn't refresh or suggests the update has failed. After a secondary site successfully updates, use the **Retry installation** option. This option doesn't reinstall the update for a secondary site that successfully installed the update, but forces the console to update the status.

Post-installation tasks

When a site installs an update, there are several tasks that can't start until after the update completes installation on the site server. This list includes the post-installation tasks that are critical for site and hierarchy operations. Because they're critical, they're actively monitored. Additional tasks that aren't directly monitored include the reinstallation of site system roles. To view the status of the critical post-installation tasks, select the **Post Installation** task while monitoring the update installation for a site.

Not all tasks complete immediately. Some tasks don't start until each site completes installation of the update. New functionality you might expect can be delayed until these tasks complete. Turning on new features doesn't start until all sites complete update installation, so new features might not be visible for some time.

The post installation tasks include:

- **Installing SMS_EXECUTIVE service**
  - Critical service that runs on the site server.
  - Reinstallation of this service should complete quickly.
- **Installing SMS_DATABASE_NOTIFICATION_MONITOR component**
  - Critical site component thread of SMS_EXECUTIVE service.
  - Reinstallation of this service should complete quickly.
- **Installing SMS_HIERARCHY_MANAGER component**
  - Critical site component that runs on the site server.
  - Responsible for reinstalling roles on site system servers. Status for individual site system role reinstallation doesn't display.
  - Reinstallation of this service should complete quickly.

  > **NOTE**
  > Some Configuration Manager site roles share the client framework. For example, the management point and pull distribution point. When these roles update, the client version on these servers updates at the same time. For more information, see How to upgrade clients.

- **Installing SMS_REPLICATION_CONFIGURATION_MONITOR component**
  - Critical site component that runs on the site server.

  - Reinstallation of this service should complete quickly.
- **Installing SMS_POLICY_PROVIDER component**
  - Critical site component that runs only on primary sites.
  - Reinstallation of this service should complete quickly.
- **Monitoring replication initialization**
  - This task only displays at the central administration site and child primary sites.
  - Dependent on the SMS_REPLICATION_CONFIGURATION_MONITOR.
  - Should complete quickly.
- **Updating Configuration Manager Client Preproduction Package**
  - This task displays even when client preproduction (also called client piloting) isn't enabled for use.
  - Doesn't start until all sites in the hierarchy finish installing the update.
- **Updating Client folder on Site Server**
  - This task doesn't display if you use the client in preproduction.
  - Should complete quickly.
- **Updating Configuration Manager Client Package**
  - This task doesn't display if you use the client in preproduction.
  - Finishes only after all sites install the update.
- **Turning on Features**
  - This task displays only at the top-tier site of the hierarchy.
  - Doesn't start until all sites in the hierarchy finish installing the update.
  - Individual features aren't displayed.

Retry installation of a failed update

When an update fails to install, review the in-console feedback to identify resolutions for warnings and errors. For more details, view the **ConfigMgrPrereq.log** on the site server. Before you retry the installation of an update, you must fix errors, and should fix warnings.

> **TIP**
> If an update has problems downloading or replicating, use the update reset tool.

When you're ready to retry the installation of an update, select the failed update, and then choose an applicable option. The update installation retry behavior depends on the node where you start the retry, and the retry option that you use.

Retry installation for the hierarchy

Retry the installation of an update for the entire hierarchy when that update is in one of the following states:

- Prerequisite checks passed with one or more warnings, and the option to ignore prerequisite check warnings wasn't set in the Update Wizard. (The update's value for **Ignore Prereq Warning** in the **Updates and Servicing** node is **No**.)
- Prerequisite failed
- Installation failed
- Replication of the content to the site failed

Go to the **Administration** workspace and select the **Updates and Servicing** node. Select the update, and then choose one of the following options:

- **Retry**: When you **Retry** from **Updates and Servicing**, the update install starts again and automatically ignores prerequisite warnings. If content replication previously failed, content for the update replicates again.
- **Ignore prerequisite warnings**: If the update install stops because of a warning, you can then choose **Ignore prerequisite warnings**. This action allows the installation of the update to continue after a few minutes, and uses the option to ignore prerequisite warnings.

Retry installation for the site

Retry the installation of an update at a specific site when that update is in one of the following states:

- Prerequisite checks passed with one or more warnings, and the option to ignore prerequisite check warnings wasn't set in the Update Wizard. (The updates value for **Ignore Prereq Warning** in the Updates and Servicing node is **No**.)
- Prerequisite failed
- Installation failed

Go to the **Monitoring** workspace, and select the **Site Servicing Status** node. Select the update, and then choose one of the following options:

- **Retry**: When you **Retry** from **Site Servicing Status**, you restart the installation of the update at only that site. Unlike running **Retry** from the **Updates and Servicing** node, this retry doesn't ignore prerequisite warnings.
- **Ignore prerequisite warnings**: If the update install stops because of a warning, you can then select **Ignore prerequisite warnings**. This action allows the installation of the update to continue after a few minutes, and uses the option to ignore prerequisite warnings.

After a site installs an update

After the site updates, review the post-update checklist for the applicable version:

- Post-update checklist for version 1906
- Post-update checklist for version 1902
- Post-update checklist for version 1810
- Post-update checklist for version 1806

Enable optional features from updates

When an update includes one or more optional features, you have the opportunity to enable those features in your hierarchy. Enable features when the update installs, or return to the console later to enable the optional features.

To view available features and their status, in the console go to the **Administration** workspace, expand **Updates and Servicing**, and select the **Features** node.

When a feature isn't optional, it's installed automatically. It doesn't appear in the**Features** node.

> **IMPORTANT**
> In a multi-site hierarchy, enable optional or pre-release features only from the central administration site. This behavior ensures there are no conflicts across the hierarchy.

When you enable a new feature or pre-release feature, the Configuration Manager hierarchy manager (HMAN) must process the change before that feature becomes available. Processing of the change is often immediate. Depending on the HMAN processing cycle, it can take up to 30 minutes to complete. After the change is processed, restart the console before you can use the feature.

List of optional features

The following features are optional in the latest version of Configuration Manager:

- Synchronize collection membership results to Azure Active Directory
- Azure Active Directory user group discovery
- Application groups
- Task sequence debugger
- Package conversion manager
- Client apps for co-managed devices
- Third-party software updates
- Approve application requests for users per device
- Support for Cisco AnyConnect 4.0.07x and later for iOS
- Device health attestation assessment for compliance policies for conditional access
- Create and run scripts
- Run task sequence step
- Task sequence content pre-caching
- Surface driver updates
- Cloud management gateway
- Data warehouse service point
- Client peer cache
- PFX create
- Azure Log Analytics connector
- Windows Defender Exploit Guard policy
- VPN for Windows 10
- Servicing a cluster-aware collection (Server groups)
- Windows Hello for Business (previously known as *Passport for Work*)
- Conditional access for managed PCs

> **TIP**
> For more information on features that require consent to enable, see pre-release features.
>
> For more information on features that are only available in the technical preview branch, see Technical Preview.

Use pre-release features from updates

The current branch includes pre-release features for early testing in a production environment. For more information, see pre-release features.

Frequently asked questions

Why don't I see certain updates in my console?

If you can't find a specific update in your console after a successful sync with the Microsoft cloud service, this behavior might be because of one of the following reasons:

- The update requires a configuration that your infrastructure doesn't use, or your current product version doesn't fulfill a prerequisite for receiving the update.

  If you think you have the required configurations and prerequisites for a missing update, confirm the service connection point is in online mode. Then, use the **Check for Updates** option in the **Updates and Servicing** node to force a check. If your service connection point is in offline mode, use the service connection tool to manually sync with the cloud service.

- Your account lacks the correct role-based administration permissions to view updates in the Configuration Manager console. For more information, see Permissions to manage updates.

Update reset tool

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Beginning with version 1706, Configuration Manager primary sites, and central administration sites include the Configuration Manager Update Reset Tool, **CMUpdateReset.exe**. Use the tool to fix issues when in-console updates have problems downloading or replicating. The tool is found in the ***\cd.latest\SMSSETUP\TOOLS*** folder of the site server.

You can use this tool with any version of the current branch that remains in support.

Use this tool when an in-console update has not yet installed and is in a failed state. A failed state means that the update download is in progress but stuck or taking an excessively long time. A long time is considered to be hours longer than your historical expectations for update packages of similar size. It can also be a failure to replicate the update to child primary sites.

When you run the tool, it runs against the update that you specify. By default, the tool does not delete successfully installed or downloaded updates.

Prerequisites

The account you use to run the tool requires the following permissions:

- **Read** and **Write** permissions to the site database of the central administration site and to each primary site in your hierarchy. To set these permissions, you can add the user account as a member of the **db_datawriter** and **db_datareader** fixed database roles on the Configuration Manager database of each site. The tool does not interact with secondary sites.
- **Local Administrator** on the top-level site of your hierarchy.
- **Local Administrator** on the computer that hosts the service connection point.

You need the GUID of the update package that you want to reset. To get the GUID:

1. In the console, go to **Administration** > **Updates and Servicing**.
2. In the display pane, right-click the heading of one of the columns (like **State**), then select **Package Guid** to add that column to the display.
3. The column now shows the update package GUID.

> **TIP**
> To copy the GUID, select the row for the update package you want to reset, and then use CTRL+C to copy that row. If you paste your copied selection into a text editor, you can then copy only the GUID for use as a command-line parameter when you run the tool.

Run the tool

The tool must be run on the top-level site of the hierarchy.

When you run the tool, use command-line parameters to specify:

- The SQL Server at the top-tier site of the hierarchy.
- The site database name at the top-tier site.
- The GUID of the update package you want to reset.

Based on the status of the update, the tool identifies the additional servers it needs to access.

If the update package is in a *post download* state, the tool does not clean up the package. As an option, you can force the removal of a successfully downloaded update by using the force delete parameter (See command-line parameters later in this topic).

After the tool runs:

- If a package was deleted, restart the SMS_Executive service at the top-tier site. Then, check for updates so you can download the package again.
- If a package was not deleted, you do not need to take any action. The update reinitializes and then restarts replication or installation.

Command-line parameters:

PARAMETER	DESCRIPTION
-S <FQDN of the SQL Server of your top-tier site>	*Required* Specify the FQDN of the SQL Server that hosts the site database for the top-tier site of your hierarchy.
-D <Database name>	*Required* Specify the name of the database at the top-tier site.
-P <Package GUID>	*Required* Specify the GUID for the update package you want to reset.
-I <SQL Server instance name>	*Optional* Identify the instance of SQL Server that hosts the site database.
-FDELETE	*Optional* Force deletion of a successfully downloaded update package.

Examples:
In a typical scenario, you want to reset an update that has download problems. Your SQL Servers FQDN is *server1.fabrikam.com*, the site database is *CM_XYZ*, and the package GUID is *61F16B3C-F1F6-4F9F-8647-2A524B0C802C*. You run: ***CMUpdateReset.exe -S server1.fabrikam.com -D CM_XYZ -P 61F16B3C-F1F6-4F9F-8647-2A524B0C802C***

In a more extreme scenario, you want to force deletion of problematic update package. Your SQL Servers FQDN is *server1.fabrikam.com*, the site database is *CM_XYZ*, and the package GUID is *61F16B3C-F1F6-4F9F-8647-2A524B0C802C*. You run: ***CMUpdateReset.exe -FDELETE -S server1.fabrikam.com -D CM_XYZ -P 61F16B3C-F1F6-4F9F-8647-2A524B0C802C***

Test the database upgrade when installing an update

6/18/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The information in this topic can help you run a test database upgrade before you install an in-console update for the current branch of Configuration Manager. However, the test upgrade is no longer a required or recommend step unless your database is suspect, or is modified by customizations not explicitly supported by Configuration Manager.

Do I need to run a test upgrade?

The deprecation of this upgrade test is made possible due to changes that are introduced with System Center Configuration Manager. These changes simplify the process and speed by which a production environment can be updated to newer versions. This redesign was done to help customers stay current with less risk, and less operational overhead when installing each new update.

The changes are to how updates install, including logic that automatically rolls back a failed update without the need to run a site recovery. These changes enable the use of the console to manage update installations, and include an option to retry installation of a failed update.

> **TIP**
> When you upgrade to System Center Configuration Manager from an older product, like System Center 2012 Configuration Manager, test database upgrades remain a recommended step.

If you still plan to test the upgrade of a site database when you install an in-console update, the following information supplements the guidance on installing an in-console update.

Prepare to run a test database upgrade

Before you install a new update in your hierarchy, like update 1702, you can test the upgrade of your site database.

To run the upgrade test, use the Configuration Manager Setup from the source files from the CD.Latest folder of a site that runs the version of Configuration Manager that you are updating to. This requirement means that to test the database update for update to 1702:

- You must have at least one site that runs version 1702 from which you can get that CD.Latest folder.
- If you do not have a site that runs the required version, consider installing a site in a lab environment, and then update that site to the new version. This creates the CD.Latest folder with the correct version of source files.

The upgrade test is run against a backup of your site database that you restored to a separate instance of SQL Server. You run Setup from the **CD.Latest** folder with the **testdbupgrade** command-line switch to test upgrade that restored copy of the database. After the test upgrade completes, the upgraded database is discarded. It cannot be used by a Configuration Manager site.

If an update install fails, you should not need to recover the site. Instead, you can retry the update installation from within the console.

Run the test upgrade

1. Use Configuration Manager Setup and the source files from the **CD.Latest** folder of a site that runs the version that you plan to update to.

2. Copy the **CD.Latest** folder to a location on the SQL Server instance that you will use to run the test database upgrade.

3. Create a backup of the site database that you want to test upgrade. Next, restore a copy of that database to an instance of SQL Server that does not host a Configuration Manager site. The SQL Server instance must use the same edition of SQL Server as your site database.

4. After you restore the database copy, run **Setup** from the CD.Latest folder that contains the source files from the version you are updating to. When you run Setup, use the **/TESTDBUPGRADE** command-line option. If the SQL Server instance that hosts the database copy is not the default instance, provide the command-line arguments to identify the instance that hosts the site database copy.

   For example, you have a site database with the database name *SMS_ABC*. You restore a copy of this site database to a supported instance of SQL Server with the instance name *DBTest*. To test an upgrade of this copy of the site database, use the following command line: **Setup.exe /TESTDBUPGRADE DBtest\CM_ABC**.

   You can find Setup.exe in the following location on the source media for System Center Configuration Manager: **SMSSETUP\BIN\X64**.

5. On the instance of SQL Server where you run the upgrade test, monitor the *ConfigMgrSetup.log* in the root of the system drive for progress and success.

   If the test upgrade fails, fix any issues related to the site database upgrade failure. Then, create a new backup of the site database and test the upgrade of the new copy of the database.

Next steps

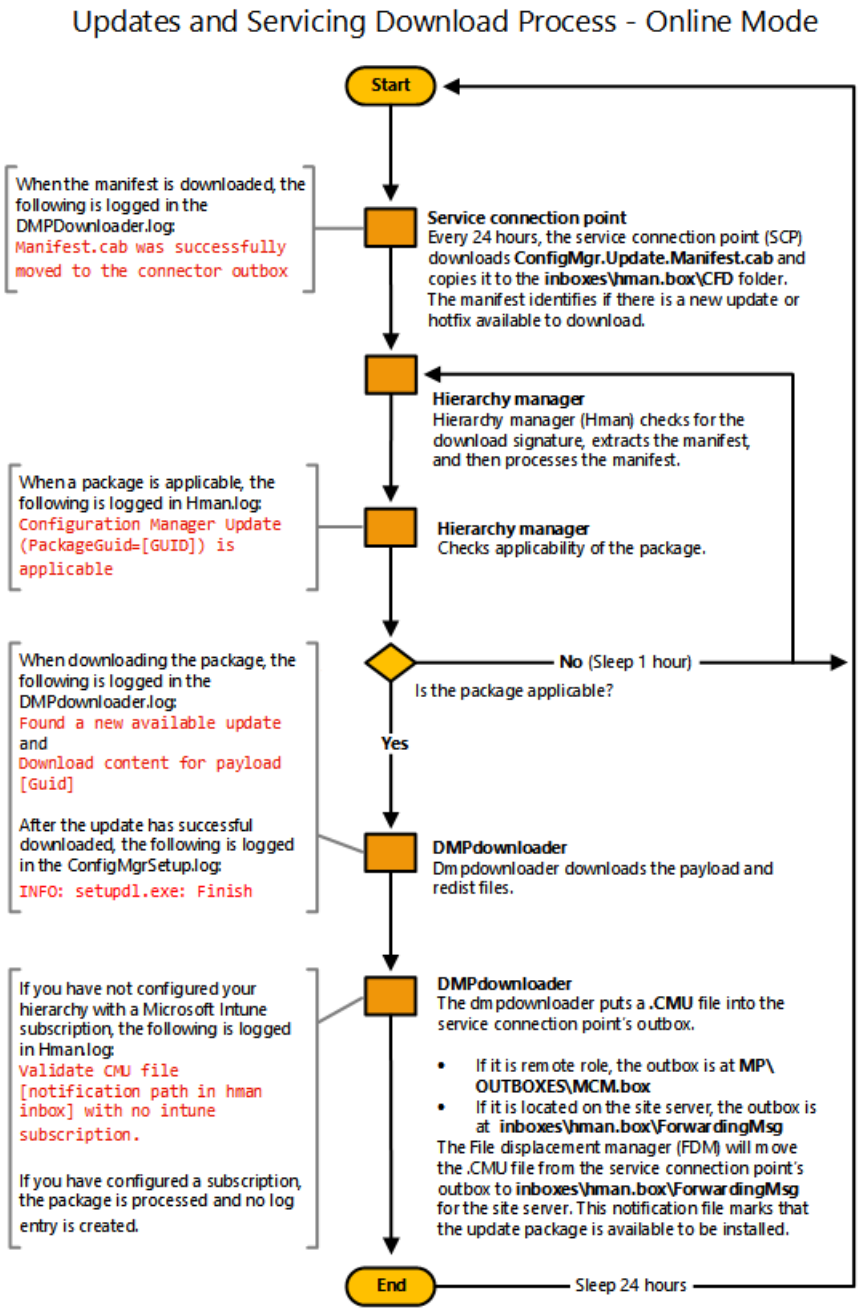
After the test database update completes successfully, discard the updated database. It cannot be used by a Configuration Manager site. You can then return to your active site and begin the update installation.

Flowchart - Download updates for System Center Configuration Manager

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This data flow displays the process by which a site with an on-line service connection point downloads in-console updates.

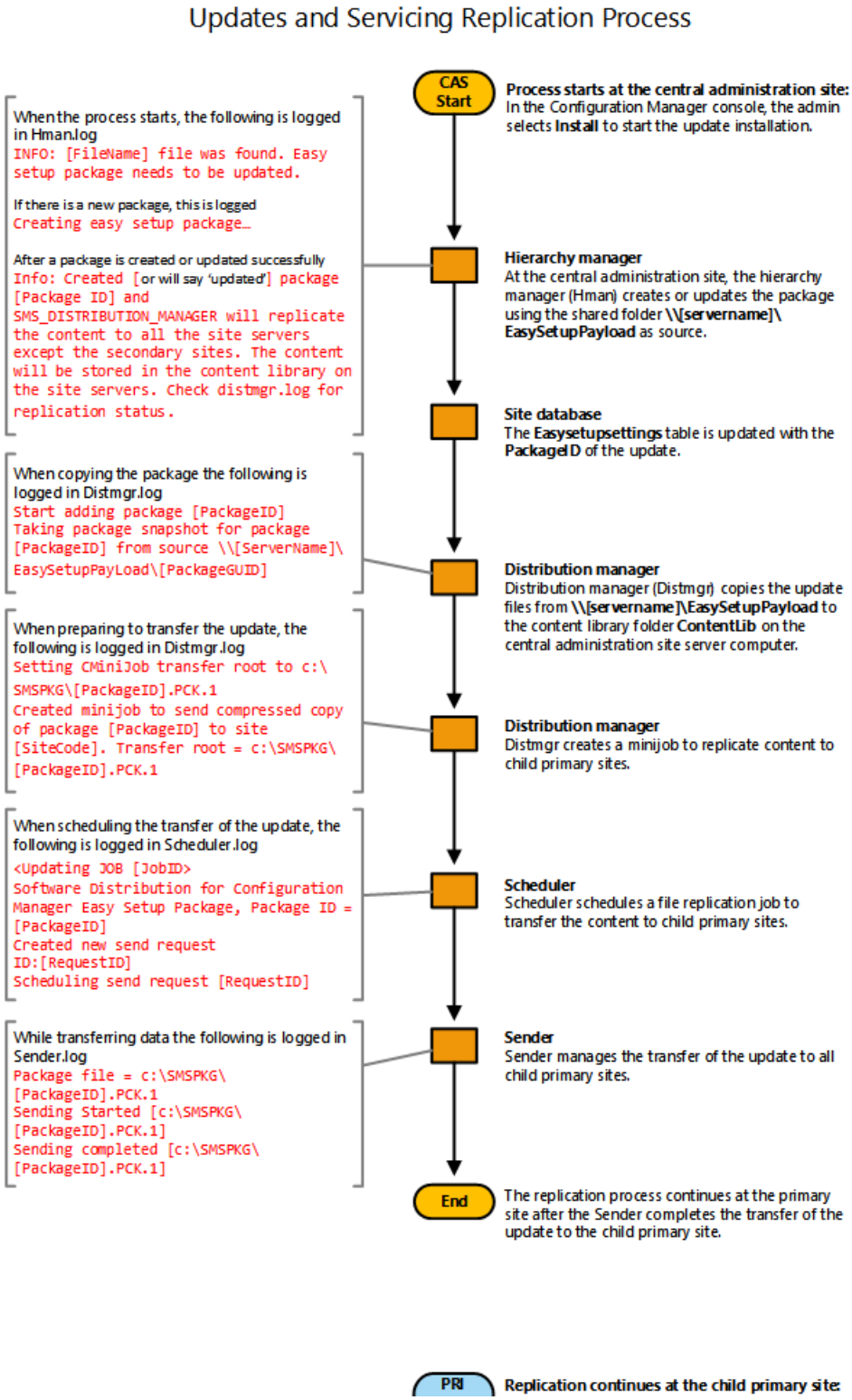


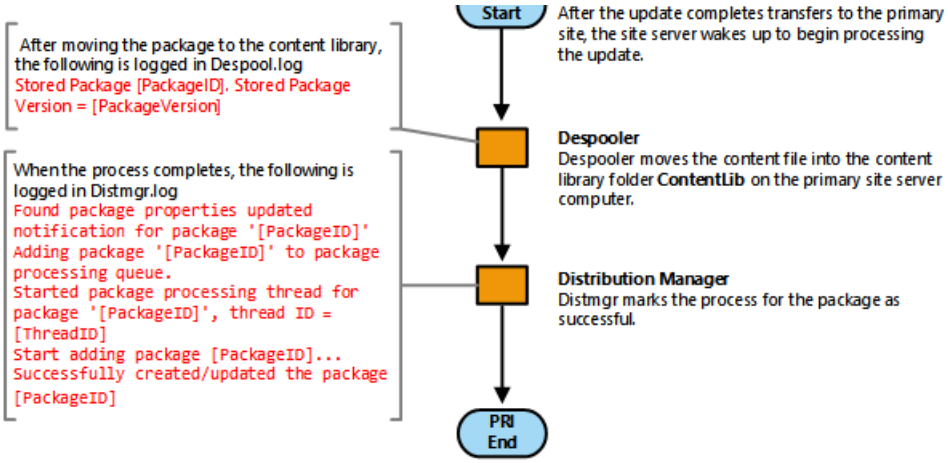
Flowchart - Update replication for System Center Configuration Manager

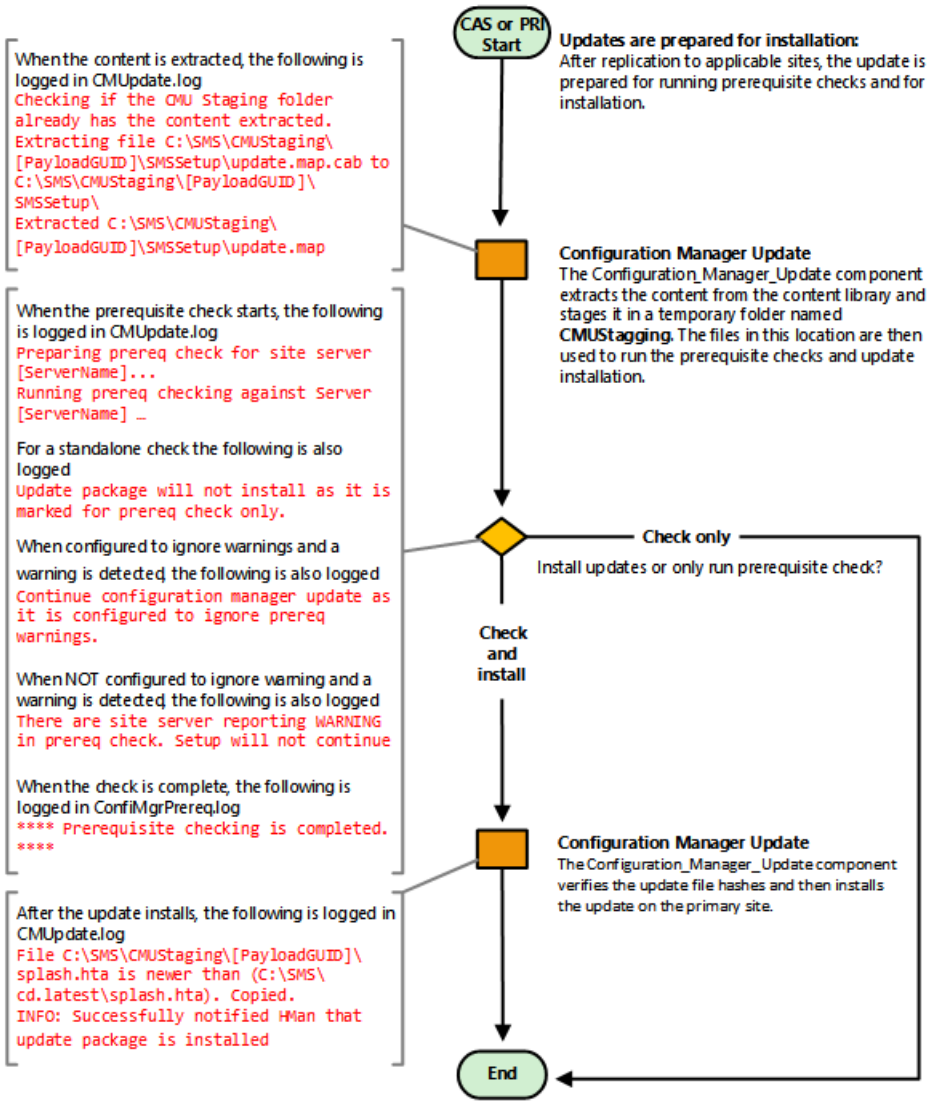
5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

These data flows display the process by which an in-console update you select to install replicates to additional sites. These flows also display the process of extracting the update to run prerequisite checks and to install updates at a central administration site and at primary sites.




Start
After the update completes transfers to the primary site, the site server wakes up to begin processing the update.
After moving the package to the content library, the following is logged in Despool.log
Stored Package [PackageID]. Stored Package Version = [PackageVersion]
Despooler
Despooler moves the content file into the content library folder ContentLib on the primary site server computer.
When the process completes, the following is logged in Distmgr.log
Found package properties updated notification for package '[PackageID]'
Adding package '[PackageID]' to package processing queue.
Started package processing thread for package '[PackageID]', thread ID = [ThreadID]
Start adding package [PackageID]...
Successfully created/updated the package [PackageID]
Distribution Manager
Distmgr marks the process for the package as successful.
PRI End


CAS or PRI Start
Updates are prepared for installation:
After replication to applicable sites, the update is prepared for running prerequisite checks and for installation.
When the content is extracted, the following is logged in CMUpdate.log
Checking if the CMU Staging folder already has the content extracted.
Extracting file C:\SMS\CMUStaging\[PayloadGUID]\SMSSetup\update.map.cab to C:\SMS\CMUStaging\[PayloadGUID]\SMSSetup\
Extracted C:\SMS\CMUStaging\[PayloadGUID]\SMSSetup\update.map
Configuration Manager Update
The Configuration_Manager_Update component extracts the content from the content library and stages it in a temporary folder named CMUStagging. The files in this location are then used to run the prerequisite checks and update installation.
When the prerequisite check starts, the following is logged in CMUpdate.log
Preparing prereq check for site server [ServerName]...
Running prereq checking against Server [ServerName] ...
For a standalone check the following is also logged
Update package will not install as it is marked for prereq check only.
When configured to ignore warnings and a warning is detected, the following is also logged
Continue configuration manager update as it is configured to ignore prereq warnings.
When NOT configured to ignore warning and a warning is detected, the following is also logged
There are site server reporting WARNING in prereq check. Setup will not continue
When the check is complete, the following is logged in ConfiMgrPrereq.log
**** Prerequisite checking is completed. ****
Check only
Install updates or only run prerequisite check?
Check and install
Configuration Manager Update
The Configuration_Manager_Update component verifies the update file hashes and then installs the update on the primary site.
After the update installs, the following is logged in CMUpdate.log
File C:\SMS\CMUStaging\[PayloadGUID]\splash.hta is newer than (C:\SMS\cd.latest\splash.hta). Copied.
INFO: Successfully notified HMan that update package is installed
End

Pre-release features in Configuration Manager

7/26/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Pre-release features are features that are in the current branch for early testing in a production environment. These features are fully supported, but still in active development. They might receive changes until they move out of the pre-release category.

Give consent

Before using pre-release features, give consent to use pre-release features. Giving consent is a one-time action per hierarchy that you can't undo. Until you give consent, you can't enable new pre-release features included with updates. After you turn on a pre-release feature, you can't turn it off.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. Click **Hierarchy Settings** in the ribbon.
3. On the **General** tab of Hierarchy Settings Properties, enable the option to **Consent to use pre-release features**. Click **OK**.

Enabling pre-release features

When you install an update that includes pre-release features, those features are visible in the Updates and Servicing Wizard with the regular features included in the update.

If you have given consent

In the Updates and Servicing Wizard, enable pre-release features. Select the pre-release features as you would any other feature.

Optionally, wait to enable pre-release features later from the **Features** node under **Updates and Servicing** in the **Administration** workspace. Select a feature, and then click **Turn on** in the ribbon. Until you give consent, this option isn't available for use.

If you haven't given consent

In the Updates and Servicing Wizard, pre-release features are visible but you can't enable them. After the update is installed, these features are visible in the **Features** node. However, you can't enable them until you give consent.

> **IMPORTANT**
>
> In a multi-site hierarchy, you can only enable optional or pre-release features from the central administration site. This behavior ensures there are no conflicts across the hierarchy.
>
> If you gave consent at a stand-alone primary site, and then expand the hierarchy by installing a new central administration site, you must give consent again at the central administration site.

When you enable a pre-release feature, the Configuration Manager hierarchy manager (HMAN) must process the change before that feature becomes available. Processing of the change is often immediate. Depending on the HMAN processing cycle, it can take up to 30 minutes to complete. After the change is processed, restart the console before using the feature.

Pre-release features

FEATURE	ADDED AS PRE-RELEASE	ADDED AS A FULL FEATURE
Task sequence debugger	Version 1906	❌
Application groups	Version 1906	❌
Azure Active Directory user group discovery	Version 1906	❌
Synchronize collection membership results to Azure Active Directory	Version 1906	❌
CMPivot standalone	Version 1906	❌
SMS Provider administration service	Version 1810	Version 1906
Enhanced HTTP site system	Version 1806	Version 1810
Client apps for co-managed devices	Version 1806	❌
SCAP extensions	Version 1806	❌
Package conversion manager	Version 1806	Version 1810
Support for Cisco AnyConnect 4.0.07x and later for iOS	Version 1802	Version 1802 with update 4163547
Phased deployments	Version 1802	Version 1806
Run task sequence step	Version 1710	Version 1802
Windows Defender Exploit Guard	Version 1710	Version 1802
Device health attestation assessment for conditional access compliance policies	Version 1710	Version 1802
Create and run Windows PowerShell scripts	Version 1706	Version 1802
Device Guard management	Version 1702	Version 1906
Cloud management gateway	Version 1610	Version 1802
Azure Log Analytics connector	Version 1606	Version 1802
Servicing a cluster-aware collection (Server groups)	Version 1602	❌

TIP

For more information on non-pre-release features that you must enable first, see Enable optional features from updates.

For more information on features that are only available in the technical preview branch, see Technical Preview.

Service windows for site servers

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can configure service windows at central administration sites and primary sites to control when in-console updates can install. You can configure multiple windows, with the window allowed for installing updates being determined by a combination of all service windows for that site server.

When no service window is configured:

- **On your top-tier site** (a central administration site or stand-alone primary site) you choose when to start the update installation.
- **On a child-primary site**, the update automatically installs after the update completes installation at the central administration site.
- **On a secondary site**, updates never start automatically. Instead, you must manually start the update installation from within the console, after the parent primary site has installed the update.

When a service window is configured:

- **On your top-tier site**, you will not be able to start the installation of any new update from within the Configuration Manager console. Even with a service window configured, the site automatically downloads updates so they are ready to install.
- **On a child-primary site**, updates that have installed at a central administration site will download to the primary site, but do not automatically start. You cannot manually start the install of an update during a time that is blocked by use of a service window. At a time when service windows no longer block update installation, the update install automatically starts.
- **Secondary sites** do not support service windows, and do not automatically install updates. After the primary parent site of a secondary site installs an update, you can start the update of the secondary site from within the console.

To configure a service window

1. In Configuration Manager console open **Administration** > **Site Configuration** > **Sites**, and then select the site server where you want to configure a service window.

2. Next, edit the site servers **Properties** and select the **Service Window** tab, where you can then set one or more service windows for that site server.

Use the Service Connection Tool for System Center Configuration Manager

9/5/2019 • 9 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the **service connection tool** when your service connection point is in offline mode, or when your Configuration Manager site system servers are not connected to the Internet. The tool can help you keep your site up-to-date with the latest updates to Configuration Manager.

When run, the tool manually connects to the Configuration Manager cloud service to upload usage information for your hierarchy, and to download updates. Uploading usage data is necessary to enable the cloud service to provide the correct updates for your deployment.

Prerequisites for using the service connection tool

The following are prerequisites, and known issues.

Prerequisites:

- You have a service connection point installed, and it is set to **Offline, on-demand connection**.
- The tool must be run from a command prompt.
- Each computer where the tool runs (the service connection point computer, and the computer that is connected to the internet) must be a x64 bit system and have the following installed:
  - Both the **Visual C++ Redistributable** x86 and x64 files. By default, Configuration Manager installs the x64 version on the computer that hosts the service connection point.

    To download a copy of the Visual C++ files, visit Visual C++ Redistributable Packages for Visual Studio 2013 at the Microsoft Download Center.
  - .NET Framework 4.5.2 or later.
- The account you use to run the tool must have:
  - **Local administrator** permissions on the computer that hosts the service connection point (where the tool is run).
  - **Read** permissions to the site database.
- You will need a USB drive with sufficient free space to store the files and updates, or another method to transfer files between the service connection point computer, and the computer that has access to the Internet. (This scenario assumes that your site and managed computers do not have a direct connection to the Internet.)

Use the service connection tool

You can find the service connection tool (**serviceconnectiontool.exe**), in the Configuration Manager installation media in **%path%\smssetup\tools\ServiceConnectionTool** folder. Always use the service connection tool that matches the version of Configuration Manager that you use.

In this procedure, the command-line examples use the following file names and folder locations (you do not need to use these paths and file names and instead can use alternatives that match your environment and preferences):

- The path to a USB Stick where data is stored for transfer between servers: **D:\USB**
- The name of the .cab file that contains data exported from your site: **UsageData.cab**
- The name of the empty folder where downloaded updates for Configuration Manager will be stored for transfer between servers: **UpdatePacks**

On the computer that hosts the service connection point:

- Open a command prompt with administrative privileges, and then change directories to the location that contains **serviceconnectiontool.exe**.

  By default, you can find this tool in the Configuration Manager installation media in **%path%\smssetup\tools\ServiceConnectionTool** folder. All of the files in this folder must be in the same folder for the service connection tool to work.

When you run the following command, the tool prepares a .cab file that contains usage information and to copies it to a location you specify. The data in the .cab file is based on the level of diagnostic usage data your site is configured to collect. (see Diagnostics and usage data for System Center Configuration Manager). Run the following command to create the .cab file:

- **serviceconnectiontool.exe -prepare -usagedatadest D:\USB\UsageData.cab**

You will also need to copy the ServiceConnectionTool folder with all of its contents to the USB drive, or otherwise make it available on the computer you will use for steps 3 and 4.

Overview

There are three primary steps to using the service connection tool

1. **Prepare**: This step runs on the computer that hosts the service connection point. When the tool is run it puts your usage data into a .cab file and stores it on a USB drive (or alternate transfer location you specify).
2. **Connect**: For this step you run the tool on a remote computer that connects to the Internet so you can upload your usage data and then download updates.
3. **Import**: This step runs on the computer that hosts the service connection point. When run, the tool imports the updates you downloaded and adds them to your site so you can then view and install those updates from the Configuration Manager console.

Beginning with version 1606, when connecting to Microsoft you can upload multiple .cab files at one time (each from a different hierarchy), and specify a proxy server and a user for the proxy server.

To upload multiple .cab files

- Place each .cab file you export from separate hierarchies into the same folder. The name of each file must be unique, and you can manually rename them if necessary.
- Then, when you run the command to upload data to Microsoft, you specify the folder that contains the .cab files. (Prior to update 1606, you could only upload data from a single hierarchy at a time, and the tool required you to specify the name of the .cab file in the folder.)
- Later, when you run the import task on the service connection point of a hierarchy, the tool automatically imports only the data for that hierarchy.

To specify a proxy server

You can use the following optional parameters to specify a proxy server (More information about using these parameters is available in the Command line parameters section of this topic):

- **-proxyserveruri [FQDN_of_proxy_server]** Use this parameter to specify the proxy server to use for this connection.
- **-proxyusername [username]** Use this parameter when you must specify a user for the proxy server.

Specify the type of updates to download

Beginning with version 1706, the tools default download behavior has changed, and the tool supports options to control what files you download.

- By default, the tool downloads only the latest available update that applies to the version of your site. It does not download hotfixes.

To modify this behavior, use one of the following parameters to change what files are downloaded.

> **NOTE**
>
> The version of your site is determined from the data in the .cab file that is uploaded when the tool runs.
>
> You can verify the version by looking for the *SiteVersion*.txt file within the .cab file.

- **-downloadall** This option downloads everything, including updates and hotfixes, regardless of the version of your site.
- **-downloadhotfix** This option downloads all hotfixes regardless of the version of your site.
- **-downloadsiteversion** This option downloads updates and hotfixes that have a version that is higher than the version of your site.

Example command line that uses *-downloadsiteversion*:

- **serviceconnectiontool.exe -connect *-downloadsiteversion* -usagedatasrc D:\USB -updatepackdest D:\USB\UpdatePacks**

To use the service connection tool

1. On the computer that hosts the service connection point:
   - Open a command prompt with administrative privileges, and then change directories to the location that contains **serviceconnectiontool.exe**.
2. Run the following command to have the tool prepare a .cab file that contains usage information and to copy it to a location you specify:
   - **serviceconnectiontool.exe -prepare -usagedatadest D:\USB\UsageData.cab**

   If you will upload .cab files from more than one hierarchy at the same time, each .cab file in the folder must have a unique name. You can manually rename files that you add to the folder.

   If you want to view the usage information that is gathered to be uploaded to the Configuration Manager cloud service, run the following command to export the same data as a .csv file which you can then view using an application like Excel:
   - **serviceconnectiontool.exe -export -dest D:\USB\UsageData.csv**
3. After the prepare step is complete, move the USB drive (or transfer the exported data by another method) to a computer that has access to the Internet.
4. On the computer with Internet access, open a command prompt with administrative privileges, and then change directories to the location that contains a copy of the tool **serviceconnectiontool.exe** and the additional files from that folder.
5. Run the following command to begin the upload of usage information and the download of updates for Configuration Manager:
   - **serviceconnectiontool.exe -connect -usagedatasrc D:\USB -updatepackdest D:\USB\UpdatePacks**

   For more examples of this command line, see the Command line options section later in this topic.

> **NOTE**
>
> When you run the command line to connect to the Configuration Manager cloud service, an error similar to the following might occur:
>
> - Unhandled Exception: System.UnauthorizedAccessException:
>
>   Access to the path 'C:\Users\br\AppData\Local\Temp\extractmanifestcab\95F8A562.sql' is denied.
>
> This error can be safely ignored and you can close the error window, and continue.

6. After the download of updates for Configuration Manager is complete, move the USB drive (or transfer the exported data by another method) to the computer that hosts the service connection point.
7. On the computer that hosts the service connection point, open a command prompt with administrative privileges, change directories to the location that contains **serviceconnectiontool.exe**, and then run the following command:
   - **serviceconnectiontool.exe -import -updatepacksrc D:\USB\UpdatePacks**
8. After the import completes, you can close the command prompt. (Only updates for the applicable hierarchy are imported).
9. Open the Configuration Manager console and navigate to **Administration** > **Updates and Servicing**. Updates that were imported are now available to install. (Prior to version 1702, Updates and Servicing was under **Administration** > **Cloud Services**.)

   For information about installing updates, see Install in-console updates for System Center Configuration Manager.

Log Files

ServiceConnectionTool.log

Each time you run the service connection tool, a log file will generate in the same location as the tool called **ServiceConnectionTool.log**. This log file will provide simple details about the execution of the tool based on what commands are used. An existing log file will be replaced each time you run the tool.

ConfigMgrSetup.log

When using the tool to connect and download updates, a log file will generate on the root of the system drive called **ConfigMgrSetup.log**. This log file will provide you with more detailed information such as what files are downloaded, extracted, and if the hash checks are successful.

Command line options

To view help information for the service connection point tool, open command prompt to the folder that contains the tool and run the command: **serviceconnectiontool.exe**.

COMMAND-LINE OPTIONS	DETAILS
-prepare -usagedatadest [drive:][path][filename.cab]	This command stores current usage data in a .cab file. Run this command as a **local administrator** on the server that hosts the service connection point. Example: **-prepare -usagedatadest D:\USB\Usagedata.cab**

COMMAND-LINE OPTIONS	DETAILS
-connect -usagedatasrc [drive:][path] -updatepackdest [drive:][path] -proxyserveruri [FQDN of proxy server] -proxyusername [username] If you use a version of Configuration Manager prior to 1606, you must specify the name of the .cab file, and cannot use the options for a proxy server. The supported command parameters are: **-connect -usagedatasrc [drive:][path][filename] -updatepackdest [drive:][path]**	This command connects to the Configuration Manager cloud service to Upload the usage data .cab files from the specified location, and to download available update packs and console content. The options for proxy servers are optional. Run this command as a **local administrator** on a computer that can connect to the Internet. Example for connecting without a proxy server: **-connect -usagedatasrc D:\USB\ -updatepackdest D:\USB\UpdatePacks** Example for connecting when you use a proxy server: **-connect -usagedatasrc D:\USB\Usagedata.cab -updatepackdest D:\USB\UpdatePacks -proxyserveruri itgproxy.redmond.corp.microsoft.com -proxyusername Meg** If you use a version prior to 1606, you must specify a file name for the .cab file, and you cannot specify a proxy server. Use the following example command line: **-connect -usagedatasrc D:\USB\Usagedata.cab -updatepackdest D:\USB\UpdatePacks**
-import -updatepacksrc [drive:][path]	This command imports the update packs and console content you previously downloaded into your Configuration Manager console. Run this command as a **local administrator** on the server that hosts the service connection point. Example: **-import -updatepacksrc D:\USB\UpdatePacks**
-export -dest [drive:][path][filename.csv]	This command exports usage data to a .csv file, which you can then view. Run this command as a **local administrator** on the server that hosts the service connection point. Example: **-export -dest D:\USB\usagedata.csv**

Use the Update Registration Tool to import hotfixes to System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Some updates for Configuration Manager are not available from the Microsoft cloud service and are only obtained out-of-band. An example is a limited release hotfix to address a specific issue.
When you must install an out-of-band release, and the update or hotfix file name ends with the extension **update.exe**, you use the **update registration tool** to manually import the update to the Configuration Manager console. The tool enables you to extract and transfer the update package to the site server, and register the update with the Configuration Manager console.

If the hotfix file has the **.exe** file extension (not **update.exe**), see Use the Hotfix Installer to install updates for System Center Configuration Manager

> **NOTE**
> This topic provides general guidance about how to install hotfixes that update System Center Configuration Manager. For details about a specific hotfix or update, refer to its corresponding Knowledge Base (KB) article at Microsoft Support.

Prerequisites for using the update registration tool:

- Only out-of-band updates that end with the **.update.exe** extension can be installed using this tool
- The tool is self-contained with the individual updates you get directly from Microsoft
- The tool does not have a dependency on the mode of the service connection point
- The tool must be run on the computer that hosts the service connection point
- The computer where the tool runs (the service connection point computer) must have the .NET Framework 4.52 installed
- The account you use to run the tool must have **local administrator** permissions on the computer that hosts the service connection point (where the tool is run)
- The account you use to run the tool must have **write** permissions to the following folder on the computer that hosts the service connection point: **<ConfigMgr Installation directory>\EasySetupPayload\offline**

To use the update registration tool

1. On the computer that hosts the service connection point:
   - Open a command prompt with administrative privileges, and then change directories to the location that contains **<Product>-<product version>-<KB article ID>-ConfigMgr.Update.exe**
2. Run the following command to start the update registration tool:
   - **<Product>-<product version>-<KB article ID>-ConfigMgr.Update.exe**

   After the hotfix is registered, it appears as a new update in the console within 24 hours. You can accelerate the process:
   - Open the Configuration Manager console and go to **Administration** > **Updates and Servicing**, and

then click **Check for Updates**. (Prior to version 1702, Updates and Servicing was under **Administration** > **Cloud Services**.)

The update registration tool logs its actions to a .log file on the local computer. The log file has the same name as the hotfix .exe file and is written to the **%SystemRoot%/Temp** folder.

After the update is registered, you can close the update registration tool.

3. Open the Configuration Manager console and navigate to **Administration** > **Updates and Servicing**. Hotfixes that were imported are now available to install. (Prior to version 1702, Updates and Servicing was under **Administration** > **Cloud Services**.)

   For information about installing updates, see Install in-console updates for System Center Configuration Manager

Use the Hotfix Installer to install updates for System Center Configuration Manager

9/5/2019 • 15 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Some updates for System Center Configuration Manager are not available from the Microsoft cloud service and are only obtained out-of-band. An example is a limited release hotfix to address a specific issue.
When you must install an update (or hotfix) that you receive from Microsoft, and that update has a file name that ends with the extension **.exe** (not **update.exe**), you use the hotfix installer that is included with that hotfix download to install the update directly to the Configuration Manager site server.

If the hotfix file has the **.update.exe** file extension, see Use the Update Registration Tool to import hotfixes to System Center Configuration Manager.

> **NOTE**
> This topic provides general guidance about how to install hotfixes that update System Center Configuration Manager. For details about a specific update, refer to its corresponding Knowledge Base (KB) article at Microsoft Support.

Overview of hotfixes for Configuration Manager

Hotfixes for Configuration Manager are similar to those for other Microsoft products, such as SQL Server, contain either one individual fix or a bundle (a rollup of fixes), and are described in a Microsoft Knowledge Base article.

Individual updates include a single focused update for a specific version of Configuration Manager.
Update bundles include multiple updates for a specific version of Configuration Manager.
When an update is a bundle, you cannot install individual updates from that bundle.

If you plan to create deployments to install updates on additional computers, you must install the update bundle on a central administration site server or primary site server.

The following happens when you run the update bundle:

- It extracts the update files for each applicable component from the update bundle.
- Starts a wizard that guides you through a process to configure the updates and deployment options for the updates.
- After you complete the wizard, the updates in the bundle that apply to the site server are installed on the site server.

The wizard also creates deployments that you can use to install the updates on additional computers. You deploy the updates to additional computers by using a supported deployment method, such as a software deployment package or Microsoft System Center Updates Publisher 2011.

When the wizard runs, it creates a **.cab** file on the site server for use with Updates Publisher 2011. Optionally, you can configure the wizard to also create one or more packages for software deployment. You can use these deployments to install updates on components, such as clients or the Configuration Manager console. You can also install updates manually on computers that do not run the Configuration Manager client.

The following three groups in Configuration Manager can be updated:

- Configuration Manager server roles, which include:
  - Central administration site
  - Primary site
  - Secondary site
  - Remote SMS Provider
- Configuration Manager console
- Configuration Manager client

> **NOTE**
>
> **Updates for site system roles** (including updates for the site database and cloud-based distribution points) are installed as part of the update for site servers and services by the site component manager.
>
> However, updates pull-distribution points are serviced by distribution manager instead of the site component manager.

Each update bundle for Configuration Manager is a self-extractable .exe file (SFX) that contains the files that are necessary to install the update on the applicable components of Configuration Manager. Typically, the SFX file can contain the following files:

FILE	DETAILS
<Product version>-QFE-KB<KB article ID>-<platform>-<language>.exe	This is the update file. The command line for this file is managed by Updatesetup.exe. For example: CM1511RTM-QFE-KB123456-X64-ENU.exe
Updatesetup.exe	This .msi wrapper manages the installation of the update bundle. When you run the update, Updatesetup.exe detects the display language of the computer where it runs. By default, the user interface for the update is in English. However, when the display language is supported, the user interface displays in the computer's local language.
License_<language>.rtf	When applicable, each update contains one or more license files for supported languages.
<Product&updatetype>-<product version>-<KB article ID>-<platform>.msp	When the update applies to the Configuration Manager console or clients, the update bundle includes separate Windows Installer patch (.msp) files. For example: **Configuration Manager console update:** ConfigMgr1511-AdminUI-KB1234567-i386.msp **Client update:** ConfigMgr1511-client-KB1234567-i386.msp ConfigMgr1511-client-KB1234567-x64.msp

By default, the update bundle logs its actions to a .log file on the site server. The log file has the same name as the update bundle and is written to the **%SystemRoot%/Temp** folder.

When you run the update bundle, it extracts a file with the same name as the update bundle to a temporary folder on the computer, and then runs Updatesetup.exe. Updatesetup.exe starts the Software Update for Configuration Manager <product version> <KB Number> Wizard.

As applicable to the scope of the update, the wizard creates a series of folders under the System Center Configuration Manager installation folder on the site server. The folder structure resembles the following: **\\<Server Name>\SMS_<Site Code>\Hotfix\<KB Number>\<Update Type>\<Platform>**.

The following table provides details about the folders in the folder structure:

FOLDER NAME	MORE INFORMATION
<Server name>	This is the name of the site server where you run the update bundle.
SMS_<Site Code>	This is the share name of the Configuration Manager installation folder.
<KB Number>	This is the ID number of the Knowledge Base article for this update bundle.
<Update type>	These are the types of updates for Configuration Manager. The wizard creates a separate folder for each type of update that is contained in the update bundle. The folder names represent the update types. They include the following: **Server**: Includes updates to site servers, site database servers, and computers that run the SMS Provider. **Client**: Includes updates to the Configuration Manager client. **AdminConsole**: Includes updates to the Configuration Manager console In addition to the preceding update types, the wizard creates a folder named **SCUP**. This folder does not represent an update type, but instead contains the .cab file for Updates Publisher.
<Platform>	This is a platform-specific folder. It contains update files that are specific to a type of processor. These folders include: - x64 - I386

How to install updates

To install updates, you must first install the update bundle on a site server. When you install an update bundle, it starts an install wizard for that update. This wizard does the following:

- Extracts the update files
- Helps you to configure deployments
- Installs applicable updates on the server components of the local computer

After you install the update bundle on a site server, you can then update additional components for Configuration Manager. The following table describes update actions for these various components:

COMPONENT	INSTRUCTIONS
Site server	Deploy updates to a remote site server when you do not choose to install the update bundle directly on that remote site server.
Site database	For remote site servers, deploy server updates that include an update to the site database if you do not install the update bundle directly on that remote site server.
Configuration Manager console	After initial installation of the Configuration Manager console, you can install updates for the Configuration Manager console on each computer that runs the console. You cannot modify the Configuration Manager console installation files to apply the updates during the initial installation of the console.
Remote SMS Provider	Install updates for each instance of the SMS Provider that runs on a computer other than the site server where you installed the update bundle.
Configuration Manager clients	After initial installation of the Configuration Manager client, you can install updates for the Configuration Manager client on each computer that runs the client.

> **NOTE**
> You can deploy updates only to computers that run the Configuration Manager client.

If you reinstall a client, Configuration Manager console, or SMS Provider, you must also reinstall the updates for these components.

Use the information in the following sections to install updates on the each of the components for Configuration Manager.

Update servers

Updates for servers can include updates for **sites**, the **site database**, and computers that run an instance of the **SMS Provider**:

Update a site

To update a Configuration Manager site, you can install the update bundle directly on the site server, or you can deploy the updates to a site server after you install the update bundle on a different site.

When you install an update on a site server, the update installation process manages additional actions that are required to apply the update, such as updating site system roles. The exception to this is the site database. The following section contains information about how to update the site database.

Update a site database

To update the site database, the installation process runs a file named **update.sql** on the site database. You can configure the update process to automatically update the site database, or you can manually update the site database later.

Automatic Update of the Site Database

When you install the update bundle on a site server, you can choose to automatically update the site database when the server update is installed. This decision applies only to the site server where you install the update bundle and does not apply to deployments that are created to install the updates on remote site servers.

> **NOTE**
> When you choose to automatically update the site database, the process updates a database regardless whether the database is located on the site server or on a remote computer.

> **IMPORTANT**
> Before you update the site database, create a backup of the site database. You cannot uninstall an update to the site database. For information about how to create a backup for Configuration Manager, see Backup and recovery for System Center Configuration Manager.

Manual Update of the Site Database

If you choose not to automatically update the site database when you install the update bundle on the site server, the server update does not modify the database on the site server where the update bundle runs. However, deployments that use the package that is created for software deployment or that installs always update the site database.

> **WARNING**
> When the update includes updates to both the site server and the site database, the update is not functional until the update is completed for both the site server and site database. Until the update is applied to the site database, the site is in an unsupported state.

To manually update a site database:

1. On the site server stop the SMS_SITE_COMPONENT_MANAGER service, and then stop the SMS_EXECUTIVE service.
2. Close the Configuration Manager console.
3. Run the update script named **update.sql** on that site's database. For information about how to run a script to update a SQL Server database, see the documentation for the version of SQL Server that you use for your site database server.
4. Restart services that were stopped in previous steps.
5. When the update bundle installs, it extracts **update.sql** to the following location on the site server: **\\<Server Name>\SMS_<Site Code>\Hotfix\<KB Number>\update.sql**

Update a computer that runs the SMS Provider

After you install an update bundle that includes updates for the SMS Provider, you must deploy the update to each computer that runs the SMS Provider. The only exception to this is the instance of the SMS Provider that was previously installed on the site server where you install the update bundle. The local instance of the SMS Provider on the site server is updated when you install the update bundle.

If you remove and then reinstall the SMS Provider on a computer, you must then reinstall the update for the SMS Provider on that computer.

Update clients

When you install an update that includes updates for the Configuration Manager client, you are presented with the option to automatically upgrade clients with the update installation, or manually upgrade clients at a later time. For more information about automatic client upgrade, see How to upgrade clients for Windows computers.

You can deploy updates with Updates Publisher or a software deployment package, or you can choose to manually

install the update on each client. For more information about how to use deployments to install updates, see the Deploy updates for Configuration Manager section in this topic.

> **IMPORTANT**
> When you install updates for clients and the update bundle includes updates for servers, be sure to also install the server updates on the primary site to which the clients are assigned.

To manually install the client update, on each Configuration Manager client, you must run **Msiexec.exe** and reference the platform-specific client update .msp file.

For example, you can use the following command line for a client update. This command line runs MSIEXEC on the client computer and references the .msp file that the update bundle extracted on the site server: **msiexec.exe /p \\<ServerName>\SMS_<SiteCode>\Hotfix\<KB Number>\Client\<Platform>\<msp> /L*v <logfile>REINSTALLMODE=mous REINSTALL=ALL**

Update Configuration Manager consoles

To update a Configuration Manager console, you must install the update on the computer that runs the console after the console installation is finished.

> **IMPORTANT**
> When you install updates for the Configuration Manager console, and the update bundle includes updates for servers, be sure to also install the server updates on the site that you use with the Configuration Manager console.

If the computer that you update runs the Configuration Manager client:

- You can use a deployment to install the update. For more information about how to use deployments to install updates, see the Deploy updates for Configuration Manager section in this topic.
- If you are logged directly on to the client computer, you can run the installation interactively.
- You can manually install the update on each computer. To manually install the Configuration Manager console update, on each computer that runs the Configuration Manager console, you can run Msiexec.exe and reference the Configuration Manager console update .msp file.

For example, you can use the following command line to update a Configuration Manager console. This command line runs MSIEXEC on the computer and references the .msp file that the update bundle extracted on the site server: **msiexec.exe /p \\<ServerName>\SMS_<SiteCode>\Hotfix\<KB Number>\AdminConsole\<Platform>\<msp> /L*v <logfile>REINSTALLMODE=mous REINSTALL=ALL**

Deploy updates for Configuration Manager

After you install the update bundle on a site server, you can use one of the following three methods to deploy updates to additional computers.

Use Updates Publisher 2011 to install updates

When you install the update bundle on a site server, the installation Wizard creates a catalog file for Updates Publisher that you can use to deploy the updates to applicable computers. The wizard always creates this catalog, even when you select the option **Use package and program to deploy this update**.

The catalog for Updates Publisher is named **SCUPCatalog.cab** and can be found in the following location on the computer where the update bundle runs: **\\<ServerName>\SMS_<SiteCode>\Hotfix\<KB Number>\SCUP\SCUPCatalog.cab**

IMPORTANT

Because the SCUPCatalog.cab file is created by using paths that are specific to the site server where the update bundle is installed, it cannot be used on other site servers.

After the wizard is finished, you can import the catalog to Updates Publisher, and then use Configuration Manager software updates to deploy the updates. For information about Updates Publisher, see Updates Publisher 2011 in the TechNet library for System Center 2012.

Use the following procedure to import the SCUPCatalog.cab file to Updates Publisher and publish the updates.

To import the updates to Updates Publisher 2011

1. Start the Updates Publisher console and click **Import**.
2. On the **Import Type** page of the Import Software Updates Catalog Wizard, select **Specify the path to the catalog to import**, and then specify the SCUPCatalog.cab file.
3. Click **Next**, and then click **Next** again.
4. In the **Security Warning - Catalog Validation** dialog box, click **Accept**. Close the wizard after it is finished.
5. In the Updates Publisher console, select the update that you want to deploy, and then click **Publish**.
6. On the **Publish Options** page of the Publish Software Updates Wizard, select **Full Content**, and then click **Next**.
7. Complete the wizard to publish the updates.

Use software deployment to install updates

When you install the update bundle on the site server of a primary site or central administration site, you can configure the installation Wizard to create update packages for software deployment. You can then deploy each package to a collection of computers that you want to update.

To create a software deployment package, on the **Configure Software Update Deployment** page of the wizard, select the check box for each update package type that you want to update. The available types can include servers, Configuration Manager consoles, and clients. A separate package is created for each type of update that you select.

NOTE

The package for servers contains updates for the following components:

- Site server
- SMS Provider
- Site database

Next, on the **Configure Software Update Deployment Method** page of the wizard, select the option **I will use software distribution**. This selection directs the wizard to create the software deployment packages.

After the wizard is finished, you can view the packages that it creates in the Configuration Manager console in the **Packages** node in the **Software Library** workspace. You can then use your standard process to deploy software packages to Configuration Manager clients. When a package runs on a client, it installs the updates to the applicable components of Configuration Manager on the client computer.

For information about how to deploy packages to Configuration Manager clients, see Packages and programs in System Center Configuration Manager.

Create collections for deploying updates to Configuration Manager

You can deploy specific updates to applicable clients. The following information can help you to create device collections for the different components for Configuration Manager.

COMPONENT OF CONFIGURATION MANAGER	INSTRUCTIONS
Central administration site server	Create a direct membership query and add the central administration site server computer.
All primary site servers	Create a direct membership query and add each primary site server computer.
All secondary site servers	Create a direct membership query and add each secondary site server computer.
All x86 clients	Create a collection with the following query criteria: **Select * from SMS_R_System inner join SMS_G_System_SYSTEM on SMS_G_System_SYSTEM.ResourceID = SMS_R_System.ResourceId where SMS_G_System_SYSTEM.SystemType = "X86-based PC"**
All x64 clients	Create a collection with the following query criteria: **Select * from SMS_R_System inner join SMS_G_System_SYSTEM on SMS_G_System_SYSTEM.ResourceID = SMS_R_System.ResourceId where SMS_G_System_SYSTEM.SystemType = "X64-based PC"**
All computers that run the Configuration Manager console	Create a direct membership query and add each computer.
Remote computers that run an instance of the SMS Provider	Create a direct membership query and add each computer.

> **NOTE**
> To update a site database, deploy the update to the site server for that site.

For information about how to create collections, see How to create collections in System Center Configuration Manager.

Checklist for installing update 1906 for Configuration Manager

8/28/2019 • 13 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

When you use the current branch of Configuration Manager, you can install the in-console update for version 1906 to update your hierarchy from a previous version.

To get the update for version 1906, you must use a service connection point at the top-level site of your hierarchy. This site system role can be in online or offline mode. After your hierarchy downloads the update package from Microsoft, find it in the console. In the **Administration** workspace, select the **Updates and Servicing** node.

- When the update is listed as **Available**, the update is ready to install. Before installing version 1906, review the following information about installing update 1906 and the checklist for configurations to make before starting the update.
- If the update displays as **Downloading** and doesn't change, review the **hman.log** and **dmpdownloader.log** for errors.
  - The dmpdownloader.log may indicate that the dmpdownloader process is waiting for an interval before checking for updates. To restart the download of the update's redistribution files, restart the **SMS_Executive** service on the site server.
  - Another common download issue occurs when proxy server settings prevent downloads from `silverlight.dlservice.microsoft.com`, `download.microsoft.com`, and `go.microsoft.com`.

For more information about installing updates, see In-console updates and servicing.

For more information about current branch versions, see Baseline and update versions.

About installing update 1906

Sites

Install update 1906 at the top-level site of your hierarchy. Start the installation from your central administration site (CAS) or from your stand-alone primary site. After the update is installed at the top-level site, child sites have the following update behavior:

- Child primary sites install the update automatically after the CAS finishes the installation of the update. You can use service windows to control when a site installs the update. For more information, see Service windows for site servers.
- Manually update each secondary site from within the Configuration Manager console after the primary parent site finishes the update installation. Automatic update of secondary site servers isn't supported.

Site system roles

When a site server installs the update, it automatically updates all of the site system roles. These roles are on the site server or installed on remote servers. Before installing the update, make sure that each site system server meets the current prerequisites for the new update version.

Configuration Manager consoles

The first time you use a Configuration Manager console after the update has finished, you're prompted to update

that console. You can also run the Configuration Manager setup on the computer that hosts the console, and choose the option to update the console. Install the update to the console as soon as possible. For more information, see Install the Configuration Manager console.

> **IMPORTANT**
>
> When you install an update at the CAS, be aware of the following limitations and delays that exist until all child primary sites also complete the update installation:
>
> - **Client upgrades** don't start. This includes automatic updates of clients and pre-production clients. Additionally, you can't promote pre-production clients to production until the last site completes the update installation. After the last site completes the update installation, client updates begin based on your configuration choices.
> - **New features** you enable with the update aren't available. This behavior is to prevent the CAS replicating data related to that feature to a site that hasn't yet installed support for that feature. After all primary sites install the update, the feature is available for use.
> - **Replication links** between the CAS and child primary sites display as not upgraded. This state displays in the update installation status as *Completed with warning* for monitoring replication initialization. In the **Monitoring** workspace of the console, this state displays as *Link is being configured*.

Early update ring

As of August 16, 2019, version 1906 is globally available for all customers to install. If you previously opted in to the early update ring, watch for an update to this current branch version.

Checklist

All sites run a supported version of Configuration Manager

Each site server in the hierarchy must run the same version of Configuration Manager before you can start the installation of update 1906. To update to 1906, you must use version 1802 or later.

Review the status of your product licensing

You must have an active Software Assurance (SA) agreement or equivalent subscription rights to install this update. When you update the site, the **Licensing** page presents the option to confirm your **Software Assurance expiration date**.

This value is optional. You can specify as a convenient reminder of your license expiration date. This date is visible when you install future updates. You might have previously specified this value during setup or installation of an update. You can also specify this value in the Configuration Manager console. In the **Administration** workspace, expand **Site Configuration**, and select **Sites**. Select **Hierarchy Settings** in the ribbon, and switch to the **Licensing** tab.

For more information, see Licensing and branches.

Review Microsoft .NET versions

When a site installs this update, if the minimum requirement of .NET Framework 4.5 isn't installed, Configuration Manager automatically installs .NET Framework 4.5.2. When this prerequisite isn't already installed, the site installs it on each server that hosts one of the following site system roles:

- Management point
- Service connection point
- Enrollment proxy point
- Enrollment point

This installation can put the site system server into a reboot pending state and report errors to the Configuration Manager component status viewer. Additionally, .NET applications on the server might experience random failures until you restart the server.

For more information, see Site and site system prerequisites.

Review the version of the Windows ADK for Windows 10

The version of the Windows 10 Assessment and Deployment Kit (ADK) should be supported for Configuration Manager version 1906. For more information on supported Windows ADK versions, see Windows 10 ADK. If you need to update the Windows ADK, do so before you begin the update of Configuration Manager. This order makes sure the default boot images are automatically updated to the latest version of Windows PE. Manually update any custom boot images after updating the site.

If you update the site before you update the Windows ADK, see Update distribution points with the boot image.

Review SQL Server Native Client version

Install a minimum version of SQL Server 2012 Native Client, which includes support for TLS 1.2. For more information, see the List of prerequisite checks.

Review the site and hierarchy status for unresolved issues

A site update can fail because of existing operational problems. Before you update a site, resolve all operational issues for the following systems:

- The site server
- The site database server
- Remote site system roles on other servers

For more information, see Use alerts and the status system.

Review file and data replication between sites

Make sure that file and database replication between sites is operational and current. Delays or backlogs in either can prevent a successful update.

Database replication

For database replication, to help resolve issues before you start the update, use the **Replication Link Analyzer** (RLA). For more information, see Monitor database replication.

Use RLA to answer the following questions:

- Is replication per group in a good state?
- Are any links degraded?
- Are there any errors?

If there's a backlog, wait until it clears out. If the backlog is large, such as millions of records, then the link is in a bad state. Before updating the site, solve the replication issue. If you need further assistance, contact Microsoft Support.

File-based replication

For file-based replication, check all inboxes for a backlog on both sending and receiving sites. If there are lots of stuck or pending replication jobs, wait until they clear out.

- On the sending site, review **sender.log**.
- On the receiving site, review **despooler log**.

Install all applicable critical Windows updates

Before you install an update for Configuration Manager, install any critical OS updates for each applicable site system. These servers include the site server, site database server, and remote site system roles. If an update that you install requires a restart, restart the applicable servers before you start the upgrade.

Disable database replicas for management points at primary sites

Configuration Manager can't successfully update a primary site that has a database replica for management points

enabled. Before you install an update for Configuration Manager, disable database replication.

For more information, see Database replicas for management points.

Set SQL Server AlwaysOn availability groups to manual failover

If you use an availability group, make sure that the availability group is set to manual failover before you start the update installation. After the site has updated, you can restore failover to be automatic. For more information, see SQL Server AlwaysOn for a site database.

Disable site maintenance tasks at each site

Before you install the update, disable any site maintenance task that might run during the time the update process is active. For example, but not limited to:

- Backup Site Server
- Delete Aged Client Operations
- Delete Aged Discovery Data

When a site database maintenance task runs during the update installation, the update installation can fail. Before you disable a task, record the schedule of the task so you can restore its configuration after the update has been installed.

For more information, see Maintenance tasks and Reference for maintenance tasks.

Temporarily stop any antivirus software

Before you update a site, stop antivirus software on the Configuration Manager servers. The antivirus software can lock some files that need to be updated which causes our update to fail.

Create a backup of the site database

Before you update a site, back up the site database at the CAS and primary sites. This backup makes sure you have a successful backup to use for disaster recovery.

For more information, see Backup and recovery.

Back up customized files

If you or a third-party product customizes any Configuration Manager configuration files, save a copy of your customizations.

For example, you add custom entries to the **osdinjection.xml** file in the `bin\X64` folder of your Configuration Manager installation directory. After you update Configuration Manager, these customizations don't persist. You need to reapply your customizations.

Plan for client piloting

When you install a site update that also updates the client, test that new client update in pre-production before you update all production clients. To use this option, configure your site to support automatic upgrades for pre-production before beginning installation of the update.

For more information, see Upgrade clients and How to test client upgrades in a pre-production collection.

Plan to use service windows

To define a period during which updates to a site server can be installed, use service windows. They can help you control when sites in your hierarchy install the update. For more information, see Service windows for site servers.

Review supported extensions

If you extend Configuration Manager with other products from Microsoft or Microsoft partners, confirm that those products support version 1906. Check with the product vendor for this information. For example, see the Microsoft Deployment Toolkit release notes.

Run the setup prerequisite checker

When the console lists the update as **Available**, you can run the prerequisite checker before installing the update. (When you install the update on the site, prerequisite checker runs again.)

To run a prerequisite check from the console, go to the **Administration** workspace, and select **Updates and Servicing**. Select the **Configuration Manager 1906** update package, and select **Run prerequisite check** in the ribbon.

For more information, see the section to **Run the prerequisite checker before installing an update** in Before you install an in-console update.

> **IMPORTANT**
> When the prerequisite checker runs, the process updates some product source files that are used for site maintenance tasks. Therefore, after running the prerequisite checker but before installing the update, if you need to perform a site maintenance task, run **Setupwpf.exe** (Configuration Manager Setup) from the CD.Latest folder on the site server.

Update sites

You're now ready to start the update installation for your hierarchy. For more information about installing the update, see Install in-console updates.

You may plan to install the update outside of normal business hours. Determine when the process will have the least effect on your business operations. Installing the update and its actions reinstall site components and site system roles.

For more information, see Updates for Configuration Manager.

Post-update checklist

After the site updates, use the following checklist to complete common tasks and configurations.

Confirm version and restart (if necessary)

Make sure each site server and site system role is updated to version 1906. In the console, add the **Version** column to the **Sites** and **Distribution Points** nodes in the **Administration** workspace. When necessary, a site system role automatically reinstalls to update to the new version.

Consider restarting remote site systems that don't successfully update at first. Review your site infrastructure and make sure that applicable site servers and remote site system servers successfully restarted. Typically, site servers restart only when Configuration Manager installs .NET as a prerequisite for a site system role.

Confirm site-to-site replication is active

In the Configuration Manager console, go to the following locations to view the status, and make sure that replication is active:

- **Monitoring** workspace, **Site Hierarchy** node
- **Monitoring** workspace, **Database Replication** node

For more information, see the following articles:

- Monitor hierarchy and replication infrastructure
- About the Replication Link Analyzer

Update Configuration Manager consoles

Update all remote Configuration Manager consoles to the same version. You're prompted to update the console when:

- You open the console.
- You go to a new node in the console.

Reconfigure database replicas for management points

After you update a primary site, reconfigure the database replica for management points that you uninstalled before you updated the site. For more information, see Database replicas for management points.

Reconfigure SQL Server AlwaysOn availability groups

If you use an availability group, reset the failover configuration to automatic. For more information, see SQL Server AlwaysOn for a site database.

Reconfigure any disabled maintenance tasks

If you disabled database maintenance tasks at a site before installing the update, reconfigure those tasks. Use the same settings that were in place before the update.

Update clients

Update clients per the plan you created, especially if you configured client piloting before installing the update. For more information, see How to upgrade clients for Windows computers.

Third-party extensions

If you use any extensions to Configuration Manager, update them to the latest version to support Configuration Manager version 1906.

Update custom boot images and media

Use the **Update Distribution Points** action for any boot image that you use, whether it's a default or custom boot image. This action makes sure that clients can use the latest version. Even if there isn't a new version of the Windows ADK, the Configuration Manager client components may change with an update. If you don't update boot images and media, task sequence deployments may fail on devices.

When you update the site, Configuration Manager automatically updates the *default* boot images. It doesn't automatically distribute the updated content to distribution points. Use the **Update Distribution Points** action on specific boot images when you're ready to distribute this content across your network.

After updating the site, manually update any *custom* boot images. This action updates the boot image with the latest client components if necessary, optionally reloads it with the current Windows PE version, and redistributes the content to the distribution points.

For more information, see Update distribution points with the boot image.

Checklist for installing update 1902 for Configuration Manager

9/5/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

When you use the current branch of Configuration Manager, you can install the in-console update for version 1902 to update your hierarchy from a previous version. (Because version 1902 is also available as baseline media, you can use the installation media to install the first site of a new hierarchy.)

To get the update for version 1902, you must use a service connection point at the top-level site of your hierarchy. This site system role can be in online or offline mode. After your hierarchy downloads the update package from Microsoft, find it in the console. In the **Administration** workspace, select the **Updates and Servicing** node.

- When the update is listed as **Available**, the update is ready to install. Before installing version 1902, review the following information about installing update 1902 and the checklist for configurations to make before starting the update.
- If the update displays as **Downloading** and doesn't change, review the **hman.log** and **dmpdownloader.log** for errors.
  - The dmpdownloader.log may indicate that the dmpdownloader process is waiting for an interval before checking for updates. To restart the download of the update's redistribution files, restart the **SMS_Executive** service on the site server.
  - Another common download issue occurs when proxy server settings prevent downloads from http://silverlight.dlservice.microsoft.com, http://download.microsoft.com/, and/or http://go.microsoft.com.

For more information about installing updates, see In-console updates and servicing.

For more information about current branch versions, see Baseline and update versions.

About installing update 1902

Sites

You install update 1902 at the top-level site of your hierarchy. Start the installation from your central administration site or from your stand-alone primary site. After the update is installed at the top-level site, child sites have the following update behavior:

- Child primary sites install the update automatically after the central administration site finishes the installation of the update. You can use service windows to control when a site installs the update. For more information, see Service windows for site servers.
- Manually update each secondary site from within the Configuration Manager console after the primary parent site finishes the update installation. Automatic update of secondary site servers isn't supported.

Site system roles

When a site server installs the update, it automatically updates all of the site system roles. These roles are on the site server or installed on remote servers. Before installing the update, make sure that each site system server meets the current prerequisites for the new update version.

Configuration Manager consoles

The first time you use a Configuration Manager console after the update has finished, you're prompted to update that console. You can also run the Configuration Manager setup on the computer that hosts the console, and choose the option to update the console. Install the update to the console as soon as possible. For more information, see Install the Configuration Manager console.

> **IMPORTANT**
>
> When you install an update at the central administration site, be aware of the following limitations and delays that exist until all child primary sites also complete the update installation:
>
> - **Client upgrades** do not start. This includes automatic updates of clients and pre-production clients. Additionally, you cannot promote pre-production clients to production until the last site completes the update installation. After the last site completes the update installation, client upgrades will begin based on your configuration choices.
> - **New features** you enable with the update are not available. This is to prevent the replication of data related to that feature from being sent to a site that has not yet installed support for that feature. After all primary sites install the update, the feature will be available for use.
> - **Replication links** between the central administration site and child primary sites display as not upgraded. This displays in the update pack installation status as a status of Completed with warning for Monitoring replication initialization. In the Monitoring node of the console, this displays as *Link is being configured*.

Checklist

All sites run a supported version of Configuration Manager

Each site server in the hierarchy must run the same version of Configuration Manager before you can start the installation of update 1902. To update to 1902, you must use version 1802, 1806, or 1810.

Review the status of your product licensing

You must have an active Software Assurance (SA) agreement or equivalent subscription rights to install this update. When you update the site, the **Licensing** page presents the option to confirm your **Software Assurance expiration date**.

This value is optional. You can specify as a convenient reminder of your license expiration date. This date is visible when you install future updates. You might have previously specified this value during setup or installation of an update. You can also specify this value in the Configuration Manager console. In the **Administration** workspace, expand **Site Configuration**, and select **Sites**. Select **Hierarchy Settings** in the ribbon, and switch to the **Licensing** tab.

For more information, see Licensing and branches.

Review Microsoft .NET versions

When a site installs this update, if the minimum requirement of .NET Framework 4.5 is not installed, Configuration Manager automatically installs .NET Framework 4.5.2. When this prerequisite isn't already installed, the site installs it on each server that hosts one of the following site system roles:

- Management point
- Service connection point
- Enrollment proxy point
- Enrollment point

This installation can put the site system server into a reboot pending state and report errors to the Configuration Manager component status viewer. Additionally, .NET applications on the server might experience random failures until the server is restarted.

For more information, see Site and site system prerequisites.

Review the version of the Windows ADK for Windows 10

The version of the Windows 10 Assessment and Deployment Kit (ADK) should be supported for Configuration Manager version 1902. For more information on supported Windows ADK versions, see Windows 10 ADK. If you need to update the Windows ADK, do so before you begin the update of Configuration Manager. This order makes sure the default boot images are automatically updated to the latest version of Windows PE. Manually update any custom boot images after updating the site.

If you update the site before you update the Windows ADK, see Update distribution points with the boot image.

Review SQL Server Native Client version

A minimum version of SQL Server 2012 Native Client which includes support for TLS 1.2 must be installed. For more information, see the List of prerequisite checks.

Review the site and hierarchy status for unresolved issues

A site update can fail due to existing operational problems. Before you update a site, resolve all operational issues for the following systems:

- The site server
- The site database server
- Remote site system roles on other servers

For more information, see Use alerts and the status system.

Review file and data replication between sites

Make sure that file and database replication between sites is operational and current. Delays or backlogs in either can prevent a smooth, successful update. For database replication, you can use the Replication Link Analyzer to help resolve issues prior to starting the update.

For more information, see About the Replication Link Analyzer.

Install all applicable critical Windows updates

Before you install an update for Configuration Manager, install any critical OS updates for each applicable site system. These servers include the site server, site database server, and remote site system roles. If an update that you install requires a restart, restart the applicable servers before you start the upgrade.

Disable database replicas for management points at primary sites

Configuration Manager can't successfully update a primary site that has a database replica for management points enabled. Before you install an update for Configuration Manager, disable database replication.

For more information, see Database replicas for management points.

Set SQL Server AlwaysOn availability groups to manual failover

If you use an availability group, make sure that the availability group is set to manual failover before you start the update installation. After the site has updated, you can restore failover to be automatic. For more information, see SQL Server AlwaysOn for a site database.

Disable site maintenance tasks at each site

Before you install the update, disable any site maintenance task that might run during the time the update process is active. For example, but not limited to:

- Backup Site Server
- Delete Aged Client Operations
- Delete Aged Discovery Data

When a site database maintenance task runs during the update installation, the update installation can fail. Before you disable a task, record the schedule of the task so you can restore its configuration after the update has been installed.

For more information, see Maintenance tasks and Reference for maintenance tasks.

Temporarily stop any antivirus software

Before you update a site, stop antivirus software on the Configuration Manager servers. The antivirus software can lock some files that need to be updated which causes our update to fail.

Create a backup of the site database

Before you update a site, back up the site database at the central administration site and primary sites. This backup makes sure you have a successful backup to use for disaster recovery.

For more information, see Backup and recovery.

Plan for client piloting

When you install an update that updates the client, you can test that new client update in pre-production before it deploys and upgrades all your active clients. To take advantage of this option, you must configure your site to support automatic upgrades for pre-production before beginning installation of the update.

For more information, see Upgrade clients and How to test client upgrades in a pre-production collection.

Plan to use service windows

To define a period during which updates to a site server can be installed, use service windows. They can help you control when sites in your hierarchy install the update. For more information, see Service windows for site servers.

Review supported extensions

If you extend Configuration Manager with other products from Microsoft or Microsoft partners, confirm that those products support version 1902. Check with the product vendor for this information. For example, see the Microsoft Deployment Toolkit release notes.

Run the setup prerequisite checker

When the update is listed in the console as **Available,** you can independently run the prerequisite checker before installing the update. (When you install the update on the site, prerequisite checker runs again.)

To run a prerequisite check from the console, go to the **Administration** workspace, and select **Updates and Servicing**. Select the **Configuration Manager 1902** update package, and select **Run prerequisite check** in the ribbon.

For more information, see the section to **Run the prerequisite checker before installing an update** in Before you install an in-console update.

> **IMPORTANT**
>
> When the prerequisite checker runs, the process updates some product source files that are used for site maintenance tasks. Therefore, after running the prerequisite checker but before installing the update, if you need to perform a site maintenance task, run **Setupwpf.exe** (Configuration Manager Setup) from the CD.Latest folder on the site server.

Update sites

You're now ready to start the update installation for your hierarchy. For more information about installing the update, see Install in-console updates.

You may plan to install the update outside of normal business hours. Determine when the process will have the least effect on your business operations. Installing the update and its actions reinstall site components and site system roles.

For more information, see Updates for Configuration Manager.

Post-update checklist

After the site updates, use the following checklist to complete common tasks and configurations.

Confirm version and restart (if necessary)

Make sure each site server and site system role has updated to version 1902. In the console, add the **Version** column to the **Sites** and **Distribution Points** nodes in the **Administration** workspace. When necessary, a site system role automatically reinstalls to update to the new version.

Consider restarting remote site systems that don't successfully update at first. Review your site infrastructure and make sure that applicable site servers and remote site system servers have restarted successfully. Typically, site servers restart only when Configuration Manager installs .NET as a prerequisite for a site system role.

Confirm site-to-site replication is active

In the Configuration Manager console, go to the following locations to view the status, and make sure that replication is active:

- **Monitoring** workspace, **Site Hierarchy** node
- **Monitoring** workspace, **Database Replication** node

For more information, see the following articles:

- Monitor hierarchy
- Monitor replication
- About the Replication Link Analyzer

Update Configuration Manager consoles

Update all remote Configuration Manager consoles to the same version. You're prompted to update the console when:

- You open the console.
- You go to a new node in the console.

Reconfigure database replicas for management points

After you update a primary site, reconfigure the database replica for management points that you uninstalled before you updated the site. For more information, see Database replicas for management points.

Reconfigure any disabled maintenance tasks

If you disabled database maintenance tasks at a site before installing the update, reconfigure those tasks. Use the same settings that were in place before the update.

Update clients

Update clients per the plan you created, especially if you configured client piloting before installing the update. For more information, see How to upgrade clients for Windows computers.

Third-party extensions

If you use any extensions to Configuration Manager, update them to the latest version to support Configuration Manager version 1902.

Update custom boot images and media

Use the **Update Distribution Points** action for any boot image that you use, whether it's a default or custom boot image. This action makes sure that clients can use the latest version. Even if there isn't a new version of the Windows ADK, the Configuration Manager client components may change with an update. If you don't update boot images and media, task sequence deployments may fail on devices.

When you update the site, Configuration Manager automatically updates the *default* boot images. It doesn't automatically distribute the updated content to distribution points. Use the **Update Distribution Points** action on specific boot images when you're ready to distribute this content across your network.

After updating the site, manually update any *custom* boot images. This action updates the boot image with the latest client components if necessary, optionally reloads it with the current Windows PE version, and redistributes the content to the distribution points.

For more information, see Update distribution points with the boot image.

Checklist for installing update 1810 for Configuration Manager

9/5/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

When you use the current branch of Configuration Manager, you can install the in-console update for version 1810 to update your hierarchy from a previous version.

To get the update for version 1810, you must use a service connection point at the top-level site of your hierarchy. This site system role can be in online or offline mode. After your hierarchy downloads the update package from Microsoft, find it in the console. In the **Administration** workspace, select the **Updates and Servicing** node.

- When the update is listed as **Available**, the update is ready to install. Before installing version 1810, review the following information about installing update 1810 and the checklist for configurations to make before starting the update.
- If the update displays as **Downloading** and doesn't change, review the **hman.log** and **dmpdownloader.log** for errors.
  - The dmpdownloader.log may indicate that the dmpdownloader process is waiting for an interval before checking for updates. To restart the download of the update's redistribution files, restart the **SMS_Executive** service on the site server.
  - Another common download issue occurs when proxy server settings prevent downloads from http://silverlight.dlservice.microsoft.com, http://download.microsoft.com/, and/or http://go.microsoft.com.

For more information about installing updates, see In-console updates and servicing.

For more information about current branch versions, see Baseline and update versions.

About installing update 1810

Sites

You install update 1810 at the top-level site of your hierarchy. Start the installation from your central administration site or from your stand-alone primary site. After the update is installed at the top-level site, child sites have the following update behavior:

- Child primary sites install the update automatically after the central administration site finishes the installation of the update. You can use service windows to control when a site installs the update. For more information, see Service windows for site servers.
- Manually update each secondary site from within the Configuration Manager console after the primary parent site finishes the update installation. Automatic update of secondary site servers isn't supported.

Site system roles

When a site server installs the update, it automatically updates all of the site system roles. These roles are on the site server or installed on remote servers. Before installing the update, make sure that each site system server meets the current prerequisites for the new update version.

Configuration Manager consoles

The first time you use a Configuration Manager console after the update has finished, you're prompted to update

that console. You can also run the Configuration Manager setup on the computer that hosts the console, and choose the option to update the console. Install the update to the console as soon as possible. For more information, see Install the Configuration Manager console.

> **IMPORTANT**
>
> When you install an update at the central administration site, be aware of the following limitations and delays that exist until all child primary sites also complete the update installation:
>
> - **Client upgrades** do not start. This includes automatic updates of clients and pre-production clients. Additionally, you cannot promote pre-production clients to production until the last site completes the update installation. After the last site completes the update installation, client upgrades will begin based on your configuration choices.
> - **New features** you enable with the update are not available. This is to prevent the replication of data related to that feature from being sent to a site that has not yet installed support for that feature. After all primary sites install the update, the feature will be available for use.
> - **Replication links** between the central administration site and child primary sites display as not upgraded. This displays in the update pack installation status as a status of Completed with warning for Monitoring replication initialization. In the Monitoring node of the console, this displays as *Link is being configured*.

Checklist

All sites run a supported version of Configuration Manager

Each site server in the hierarchy must run the same version of Configuration Manager before you can start the installation of update 1810. To update to 1810, you must use version 1710, 1802, or 1806.

Review the status of your product licensing

You must have an active Software Assurance (SA) agreement or equivalent subscription rights to install this update. When you update the site, the **Licensing** page presents the option to confirm your **Software Assurance expiration date**.

This value is optional. You can specify as a convenient reminder of your license expiration date. This date is visible when you install future updates. You might have previously specified this value during setup or installation of an update. You can also specify this value in the Configuration Manager console. In the **Administration** workspace, expand **Site Configuration**, and select **Sites**. Click **Hierarchy Settings** in the ribbon, and switch to the **Licensing** tab.

For more information, see Licensing and branches.

Review Microsoft .NET versions

When a site installs this update, if the minimum requirement of .NET Framework 4.5 is not installed, Configuration Manager automatically installs .NET Framework 4.5.2. When this prerequisite isn't already installed, the site installs it on each server that hosts one of the following site system roles:

- Management point
- Service connection point
- Enrollment proxy point
- Enrollment point

This installation can put the site system server into a reboot pending state and report errors to the Configuration Manager component status viewer. Additionally, .NET applications on the server might experience random failures until the server is restarted.

For more information, see Site and site system prerequisites.

Review the version of the Windows ADK for Windows 10

The version of the Windows 10 Assessment and Deployment Kit (ADK) should be supported for Configuration

Manager version 1810. For more information on supported Windows ADK versions, see Windows 10 ADK. If you need to update the Windows ADK, do so before you begin the update of Configuration Manager. This order makes sure the default boot images are automatically updated to the latest version of Windows PE. Manually update any custom boot images after updating the site.

If you update the site before you update the Windows ADK, see Update distribution points with the boot image.

Review SQL Server Native Client version

A minimum version of SQL Server 2012 Native Client which includes support for TLS 1.2 must be installed. For more information, see the List of prerequisite checks.

Review the site and hierarchy status for unresolved issues

A site update can fail due to existing operational problems. Before you update a site, resolve all operational issues for the following systems:

- The site server
- The site database server
- Remote site system roles on other servers

For more information, see Use alerts and the status system.

Review file and data replication between sites

Make sure that file and database replication between sites is operational and current. Delays or backlogs in either can prevent a smooth, successful update. For database replication, you can use the Replication Link Analyzer to help resolve issues prior to starting the update.

For more information, see About the Replication Link Analyzer.

Install all applicable critical Windows updates

Before you install an update for Configuration Manager, install any critical OS updates for each applicable site system. These servers include the site server, site database server, and remote site system roles. If an update that you install requires a restart, restart the applicable servers before you start the upgrade.

Disable database replicas for management points at primary sites

Configuration Manager can't successfully update a primary site that has a database replica for management points enabled. Before you install an update for Configuration Manager, disable database replication.

For more information, see Database replicas for management points.

Set SQL Server AlwaysOn availability groups to manual failover

If you use an availability group, make sure that the availability group is set to manual failover before you start the update installation. After the site has updated, you can restore failover to be automatic. For more information, see SQL Server AlwaysOn for a site database.

Disable site maintenance tasks at each site

Before you install the update, disable any site maintenance task that might run during the time the update process is active. For example, but not limited to:

- Backup Site Server
- Delete Aged Client Operations
- Delete Aged Discovery Data

When a site database maintenance task runs during the update installation, the update installation can fail. Before you disable a task, record the schedule of the task so you can restore its configuration after the update has been installed.

For more information, see Maintenance tasks and Reference for maintenance tasks.

Temporarily stop any antivirus software

Before you update a site, stop antivirus software on the Configuration Manager servers.

Create a backup of the site database

Before you update a site, back up the site database at the central administration site and primary sites. This backup makes sure you have a successful backup to use for disaster recovery.

For more information, see Backup and recovery.

Plan for client piloting

When you install an update that updates the client, you can test that new client update in pre-production before it deploys and upgrades all your active clients. To take advantage of this option, you must configure your site to support automatic upgrades for pre-production before beginning installation of the update.

For more information, see Upgrade clients and How to test client upgrades in a pre-production collection.

Plan to use service windows

To define a period during which updates to a site server can be installed, use service windows. They can help you control when sites in your hierarchy install the update. For more information, see Service windows for site servers.

Review supported extensions

If you extend Configuration Manager with other products from Microsoft or Microsoft partners, confirm that those products support version 1810. Check with the product vendor for this information. For example, see the Microsoft Deployment Toolkit release notes.

Run the setup prerequisite checker

When the update is listed in the console as **Available,** you can independently run the prerequisite checker before installing the update. (When you install the update on the site, prerequisite checker runs again.)

To run a prerequisite check from the console, go to the **Administration** workspace, and select **Updates and Servicing**. Select the **Configuration Manager 1810** update package, and click **Run prerequisite check** in the ribbon.

For more information, see the section to **Run the prerequisite checker before installing an update** in Before you install an in-console update.

> **IMPORTANT**
>
> When the prerequisite checker runs, the process updates some product source files that are used for site maintenance tasks. Therefore, after running the prerequisite checker but before installing the update, if you need to perform a site maintenance task, run **Setupwpf.exe** (Configuration Manager Setup) from the CD.Latest folder on the site server.

Update sites

You're now ready to start the update installation for your hierarchy. For more information about installing the update, see Install in-console updates.

You may plan to install the update outside of normal business hours. Determine when the process will have the least effect on your business operations. Installing the update and its actions reinstall site components and site system roles.

For more information, see Updates for Configuration Manager.

Post-update checklist

After the site updates, use the following checklist to complete common tasks and configurations.

Confirm version and restart (if necessary)

Make sure each site server and site system role has updated to version 1810. In the console, add the **Version** column to the **Sites** and **Distribution Points** nodes in the **Administration** workspace. When necessary, a site

system role automatically reinstalls to update to the new version.

Consider restarting remote site systems that don't successfully update at first. Review your site infrastructure and make sure that applicable site servers and remote site system servers have restarted successfully. Typically, site servers restart only when Configuration Manager installs .NET as a prerequisite for a site system role.

Confirm site-to-site replication is active

In the Configuration Manager console, go to the following locations to view the status, and make sure that replication is active:

- **Monitoring** workspace, **Site Hierarchy** node
- **Monitoring** workspace, **Database Replication** node

For more information, see the following articles:

- Monitor hierarchy
- Monitor replication
- About the Replication Link Analyzer

Update Configuration Manager consoles

Update all remote Configuration Manager consoles to the same version. You're prompted to update the console when:

- You open the console.
- You go to a new node in the console.

Reconfigure database replicas for management points

After you update a primary site, reconfigure the database replica for management points that you uninstalled before you updated the site. For more information, see Database replicas for management points.

Reconfigure any disabled maintenance tasks

If you disabled database maintenance tasks at a site before installing the update, reconfigure those tasks. Use the same settings that were in place before the update.

Update clients

Update clients per the plan you created, especially if you configured client piloting before installing the update. For more information, see How to upgrade clients for Windows computers.

Third-party extensions

If you use any extensions to Configuration Manager, update them to the latest version to support Configuration Manager version 1810.

Update custom boot images and media

Use the **Update Distribution Points** action for any boot image that you use, whether it's a default or custom boot image. This action makes sure that clients can use the latest version. Even if there isn't a new version of the Windows ADK, the Configuration Manager client components may change with an update. If you don't update boot images and media, task sequence deployments may fail on devices.

When you update the site, Configuration Manager automatically updates the *default* boot images. It doesn't automatically distribute the updated content to distribution points. Use the **Update Distribution Points** action on specific boot images when you're ready to distribute this content across your network.

After updating the site, manually update any *custom* boot images. This action updates the boot image with the latest client components if necessary, optionally reloads it with the current Windows PE version, and redistributes the content to the distribution points.

For more information, see Update distribution points with the boot image.

Checklist for installing update 1806 for Configuration Manager

9/5/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

When you use the current branch of Configuration Manager, you can install the in-console update for version 1806 to update your hierarchy from a previous version.

To get the update for version 1806, you must use a service connection point at the top-level site of your hierarchy. This site system role can be in online or offline mode. After your hierarchy downloads the update package from Microsoft, find it in the console. In the **Administration** workspace, select the **Updates and Servicing** node.

- When the update is listed as **Available**, the update is ready to install. Before installing version 1806, review the following information about installing update 1806 and the checklist for configurations to make before starting the update.
- If the update displays as **Downloading** and doesn't change, review the **hman.log** and **dmpdownloader.log** for errors.
  - The dmpdownloader.log may indicate that the dmpdownloader process is waiting for an interval before checking for updates. To restart the download of the update's redistribution files, restart the **SMS_Executive** service on the site server.
  - Another common download issue occurs when proxy server settings prevent downloads from http://silverlight.dlservice.microsoft.com and http://download.microsoft.com/.

For more information about installing updates, see In-console updates and servicing.

For more information about current branch versions, see Baseline and update versions.

About installing update 1806

Sites

You install update 1806 at the top-level site of your hierarchy. Start the installation from your central administration site or from your stand-alone primary site. After the update is installed at the top-level site, child sites have the following update behavior:

- Child primary sites install the update automatically after the central administration site finishes the installation of the update. You can use service windows to control when a site installs the update. For more information, see Service windows for site servers.
- Manually update each secondary site from within the Configuration Manager console after the primary parent site finishes the update installation. Automatic update of secondary site servers isn't supported.

Site system roles

When a site server installs the update, it automatically updates all of the site system roles. These roles are on the site server or installed on remote servers. Before installing the update, make sure that each site system server meets the current prerequisites for the new update version.

Configuration Manager consoles

The first time you use a Configuration Manager console after the update has finished, you're prompted to update that console. You can also run the Configuration Manager setup on the computer that hosts the console, and

choose the option to update the console. Install the update to the console as soon as possible. For more information, see Install the Configuration Manager console.

> **IMPORTANT**
>
> When you install an update at the central administration site, be aware of the following limitations and delays that exist until all child primary sites also complete the update installation:
>
> - **Client upgrades** do not start. This includes automatic updates of clients and pre-production clients. Additionally, you cannot promote pre-production clients to production until the last site completes the update installation. After the last site completes the update installation, client upgrades will begin based on your configuration choices.
> - **New features** you enable with the update are not available. This is to prevent the replication of data related to that feature from being sent to a site that has not yet installed support for that feature. After all primary sites install the update, the feature will be available for use.
> - **Replication links** between the central administration site and child primary sites display as not upgraded. This displays in the update pack installation status as a status of Completed with warning for Monitoring replication initialization. In the Monitoring node of the console, this displays as *Link is being configured*.

Checklist

All sites run a supported version of Configuration Manager

Each site server in the hierarchy must run the same version of Configuration Manager before you can start the installation of update 1806. To update to 1806, you must use version 1706, 1710, or 1802.

Review the status of your product licensing

You must have an active Software Assurance (SA) agreement or equivalent subscription rights to install this update. When you update the site, the **Licensing** page presents the option to confirm your **Software Assurance expiration date**.

This value is optional. You can specify as a convenient reminder of your license expiration date. This date is visible when you install future updates. You might have previously specified this value during setup or installation of an update. You can also specify this value in the Configuration Manager console. In the **Administration** workspace, expand **Site Configuration**, and select **Sites**. Click **Hierarchy Settings** in the ribbon, and switch to the **Licensing** tab.

For more information, see Licensing and branches.

Review Microsoft .NET versions

When a site installs this update, Configuration Manager automatically installs .NET Framework 4.5.2. When this prerequisite isn't already installed, the site installs it on each server that hosts one of the following site system roles:

- Management point
- Service connection point
- Enrollment proxy point
- Enrollment point

This installation can put the site system server into a reboot pending state and report errors to the Configuration Manager component status viewer. Additionally, .NET applications on the server might experience random failures until the server is restarted.

For more information, see Site and site system prerequisites.

Review the version of the Windows ADK for Windows 10

The version of the Windows 10 Assessment and Deployment Kit (ADK) should be supported for Configuration Manager version 1806. For more information on supported Windows ADK versions, see Windows 10 ADK. If you need to update the Windows ADK, do so before you begin the update of Configuration Manager. This order

ensures the default boot images are automatically updated to the latest version of Windows PE. Manually update any custom boot images after updating the site.

If you update the site before you update the Windows ADK, see Update distribution points with the boot image.

Review the site and hierarchy status for unresolved issues

Before you update a site, resolve all operational issues for the site server, the site database server, and site system roles that are installed on remote computers. A site update can fail due to existing operational problems.

For more information, see Use alerts and the status system.

Review file and data replication between sites

Ensure that file and database replication between sites is operational and current. Delays or backlogs in either can prevent a smooth, successful update. For database replication, you can use the Replication Link Analyzer to help resolve issues prior to starting the update.

For more information, see About the Replication Link Analyzer.

Install all applicable critical Windows updates

Before you install an update for Configuration Manager, install any critical OS updates for each applicable site system. These servers include the site server, site database server, and remote site system roles. If an update that you install requires a restart, restart the applicable servers before you start the upgrade.

Disable database replicas for management points at primary sites

Configuration Manager can't successfully update a primary site that has a database replica for management points enabled. Before you install an update for Configuration Manager, disable database replication.

For more information, see Database replicas for management points.

Set SQL Server AlwaysOn availability groups to manual failover

If you use an availability group, ensure that the availability group is set to manual failover before you start the update installation. After the site has updated, you can restore failover to be automatic. For more information, see SQL Server AlwaysOn for a site database.

Disable site maintenance tasks at each site

Before you install the update, disable any site maintenance task that might run during the time the update process is active. For example, but not limited to:

- Backup Site Server
- Delete Aged Client Operations
- Delete Aged Discovery Data

When a site database maintenance task runs during the update installation, the update installation can fail. Before you disable a task, record the schedule of the task so you can restore its configuration after the update has been installed.

For more information, see Maintenance tasks and Reference for maintenance tasks.

Temporarily stop any antivirus software

Before you update a site, stop antivirus software on the Configuration Manager servers.

Create a backup of the site database

Before you update a site, back up the site database at the central administration site and primary sites. This backup ensures that you have a successful backup to use for disaster recovery.

For more information, see Backup and recovery.

Plan for client piloting

When you install an update that updates the client, you can test that new client update in pre-production before it deploys and upgrades all your active clients. To take advantage of this option, you must configure your site to

support automatic upgrades for pre-production before beginning installation of the update.

For more information, see Upgrade clients and How to test client upgrades in a pre-production collection.

Plan to use service windows

To define a period during which updates to a site server can be installed, use service windows. They can help you control when sites in your hierarchy install the update. For more information, see Service windows for site servers.

Review supported extensions

If you extend Configuration Manager with other products from Microsoft or Microsoft partners, confirm that those products support version 1806. Check with the product vendor for this information. For example, see the Microsoft Deployment Toolkit release notes.

Run the setup prerequisite checker

When the update is listed in the console as **Available,** you can independently run the prerequisite checker before installing the update. (When you install the update on the site, prerequisite checker runs again.)

To run a prerequisite check from the console, go to the **Administration** workspace, and select **Updates and Servicing**. Select the **Configuration Manager 1806** update package, and click **Run prerequisite check** in the ribbon.

For more information, see the section to **Run the prerequisite checker before installing an update** in Before you install an in-console update.

> **IMPORTANT**
> When the prerequisite checker runs, the process updates some product source files that are used for site maintenance tasks. Therefore, after running the prerequisite checker but before installing the update, if you need to perform a site maintenance task, run **Setupwpf.exe** (Configuration Manager Setup) from the CD.Latest folder on the site server.

Update sites

You're now ready to start the update installation for your hierarchy. For more information about installing the update, see Install in-console updates.

You may plan to install the update outside of normal business hours. Determine when the process will have the least effect on your business operations. Installing the update and its actions reinstall site components and site system roles.

For more information, see Updates for Configuration Manager.

Post-update checklist

After the site updates, use the following checklist to complete common tasks and configurations.

Confirm version and restart (if necessary)

Make sure each site server and site system role has updated to version 1806. In the console, add the **Version** column to the **Sites** and **Distribution Points** nodes in the **Administration** workspace. When necessary, a site system role automatically reinstalls to update to the new version.

Consider restarting remote site systems that don't successfully update at first. Review your site infrastructure and make sure that applicable site servers and remote site system servers have restarted successfully. Typically, site servers restart only when Configuration Manager installs .NET as a prerequisite for a site system role.

Confirm site-to-site replication is active

In the Configuration Manager console, go to the following locations to view the status, and make sure that replication is active:

- **Monitoring** workspace, **Site Hierarchy** node

- **Monitoring** workspace, **Database Replication** node

For more information, see the following articles:

- Monitor hierarchy
- Monitor replication
- About the Replication Link Analyzer

Update Configuration Manager consoles

Update all remote Configuration Manager consoles to the same version. You're prompted to update the console when:

- You open the console.
- You go to a new node in the console.

Reconfigure database replicas for management points

After you update a primary site, reconfigure the database replica for management points that you uninstalled before you updated the site. For more information, see Database replicas for management points.

Reconfigure any disabled maintenance tasks

If you disabled database maintenance tasks at a site before installing the update, reconfigure those tasks. Use the same settings that were in place before the update.

Update clients

Update clients per the plan you created, especially if you configured client piloting before installing the update. For more information, see How to upgrade clients for Windows computers.

Third-party extensions

If you use any extensions to Configuration Manager, update them to the latest version to support Configuration Manager version 1806.

Update custom boot images and media

Use the **Update Distribution Points** action for any boot image that you use, whether its a default or custom boot image. This action makes sure that clients can use the latest version. Even if there isn't a new version of the Windows ADK, the Configuration Manager client components may change with an update. If you don't update boot images and media, task sequence deployments may fail on devices.

When you update the site, Configuration Manager automatically updates the *default* boot images. It doesn't automatically distribute the updated content to distribution points. Use the **Update Distribution Points** action on specific boot images when you're ready to distribute this content across your network.

After updating the site, manually update any *custom* boot images. This action updates the boot image with the latest client components if necessary, optionally reloads it with the current Windows PE version, and redistributes the content to the distribution points.

For more information, see Update distribution points with the boot image.

Checklist for installing update 1802 for System Center Configuration Manager

8/12/2019 • 10 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

When you use the current branch of System Center Configuration Manager, you can install the in-console update for version 1802 to update your hierarchy from a previous version. (Because version 1802 is also available as baseline media, you can use the installation media to install the first site of a new hierarchy.)

To get the update for version 1802, you must use a service connection point at the top-level site of your hierarchy. This site system role can be in online or offline mode. After your hierarchy downloads the update package from Microsoft, you can find it in the console under the **Administration** workspace in the **Updates and Servicing** node.

- When the update is listed as **Available**, the update is ready to install. Before installing version 1802, review the following information about installing update 1802 and the checklist for configurations to make before starting the update.
- If the update displays as **Downloading** and does not change, review the **hman.log** and **dmpdownloader.log** for errors.
    - If the dmpdownloader.log indicates the dmpdownloader process is asleep and waiting for an interval before checking for updates, you can restart the **SMS_Executive** service on the site server to restart the download of the update's redistribution files.
    - Another common download issue occurs when proxy server settings prevent downloads from http://silverlight.dlservice.microsoft.com and http://download.microsoft.com.

For more information about installing updates, see In-console updates and servicing.

For information about the versions of the Current Branch, see Baseline and update versions in Updates for System Center Configuration Manager.

About installing update 1802

Sites:
You install update 1802 at the top-level site of your hierarchy. This means you initiate the installation from your central administration site if you have one, or from your stand-alone primary site. After the update is installed at the top-tier site, child sites have the following update behavior:

- Child primary sites install the update automatically after the central administration site finishes the installation of the update. You can use service windows to control when a site installs the update. For more information, see Service windows for site servers.
- You must manually update each secondary site from within the Configuration Manager console after the primary parent site finishes the update installation. Automatic update of secondary site servers is not supported.

Site system roles:
When a site server installs the update, the site system roles that are installed on the site server computer, and those that are installed on remote computers, automatically get updated. Before installing the update, make sure that

each site system server meets the prerequisites for operation with the new update version.

Configuration Manager consoles:
The first time you use a Configuration Manager console after the update has finished, you will be prompted to update that console. To do so, you must run Configuration Manager setup on the computer that hosts the console, and then choose the option to update the console. We recommend that you do not delay installing the update to the console.

> **IMPORTANT**
> When you install an update at the central administration site, be aware of the following limitations and delays that exist until all child primary sites also complete the update installation:
>
> - **Client upgrades** do not start. This includes automatic updates of clients and pre-production clients. Additionally, you cannot promote pre-production clients to production until the last site completes the update installation. After the last site completes the update installation, client upgrades will begin based on your configuration choices.
> - **New features** you enable with the update are not available. This is to prevent the replication of data related to that feature from being sent to a site that has not yet installed support for that feature. After all primary sites install the update, the feature will be available for use.
> - **Replication links** between the central administration site and child primary sites display as not upgraded. This displays in the update pack installation status as a status of Completed with warning for Monitoring replication initialization. In the Monitoring node of the console, this displays as *Link is being configured*.

Checklist

Ensure that all sites run a version of System Center Configuration Manager that supports update to 1802:
Each site server in the hierarchy must run the same version of System Center Configuration Manager before you can start the installation of update 1802. To update to 1802, you must use version 1702, 1706, or 1710.

Review the status of your Software Assurance or equivalent subscription rights:
You must have an active Software Assurance (SA) agreement to install update 1802. When you install this update, the **Licensing** tab presents the option to confirm your **Software Assurance expiration date**.

This is an optional value that you can specify as a convenient reminder of your license expiration date. This date is visible when you install future updates. You might have previously specified this value during setup or installation of an update, or by using the **Licensing** tab of the **Hierarchy Settings**, from within the Configuration Manager console.

For more information, see Licensing and branches for System Center Configuration Manager.

Review installed Microsoft .NET versions on site system servers: When a site installs this update, Configuration Manager automatically installs .NET Framework 4.5.2 on each computer that hosts one of the following site system roles when .NET Framework 4.5 or later is not already installed:

- Enrollment proxy point
- Enrollment point
- Management point
- Service connection point

This installation can put the site system server into a reboot pending state and report errors to the Configuration Manager component status viewer. Additionally, .NET applications on the server might experience random failures until the server is restarted.

For more information, see Site and site system prerequisites.

Review the version of the Windows Assessment and Deployment Kit (ADK) for Windows 10 The Windows 10 ADK should be version 1703 or later. (For more information on supported Windows ADK versions, see Windows 10 ADK.) If you must update the Windows ADK, do so before you begin the update of Configuration Manager. This ensures the default boot images are automatically updated to the latest version of Windows PE. (Custom boot images must be updated manually.)

If you update the site before you update the Windows ADK, see Update distribution points with the boot image.

Review the site and hierarchy status and verify that there are no unresolved issues: Before you update a site, resolve all operational issues for the site server, the site database server, and site system roles that are installed on remote computers. A site update can fail due to existing operational problems.

For more information, see Use alerts and the status system for System Center Configuration Manager.

Review file and data replication between sites:
Ensure that file and database replication between sites is operational and current. Delays or backlogs in either can prevent a smooth, successful update. For database replication, you can use the Replication Link Analyzer to help resolve issues prior to starting the update.

For more information, see About the Replication Link Analyzer.

Install all applicable critical updates for operating systems on computers that host the site, the site database server, and remote site system roles: Before you install an update for Configuration Manager, install any critical updates for each applicable site system. If an update that you install requires a restart, restart the applicable computers before you start the upgrade.

Disable database replicas for management points at primary sites:
Configuration Manager cannot successfully update a primary site that has a database replica for management points enabled. Disable database replication before you install an update for Configuration Manager.

For more information, see Database replicas for management points for System Center Configuration Manager.

Set SQL Server AlwaysOn availability groups to manual failover:
If you use an availability group, ensure that the availability group is set to manual failover before you start the update installation. After the site has updated, you can restore failover to be automatic. For more information see SQL Server AlwaysOn for a site database.

Reconfigure software update points that use NLBs:

Configuration Manager cannot update a site that uses a network load balancing (NLB) cluster to host software update points.

If you use NLB clusters for software update points, use Windows PowerShell to remove the NLB cluster. For more information, see Plan for software updates in System Center Configuration Manager.

Disable all site maintenance tasks at each site for the duration of the update installation on that site:
Before you install the update, disable any site maintenance task that might run during the time the update process is active. This includes but is not limited to the following:

- Backup Site Server
- Delete Aged Client Operations
- Delete Aged Discovery Data

When a site database maintenance task runs during the update installation, the update installation can fail. Before you disable a task, record the schedule of the task so you can restore its configuration after the update has been installed.

For more information, see Maintenance tasks for System Center Configuration Manager and Reference for maintenance tasks for System Center Configuration Manager.

Temporarily stop any antivirus software on the System Center Configuration Manager servers: Before you update a site, ensure that you have stopped antivirus software on the Configuration Manager servers.

Create a backup of the site database at the central administration site and primary sites: Before you update a site, back up the site database to ensure that you have a successful backup to use for disaster recovery.

For more information, see Backup and recovery for System Center Configuration Manager.

Plan for client piloting:
When you install an update that updates the client, you can test that new client update in pre-production before it deploys and upgrades all your active clients.

To take advantage of this option, you must configure your site to support automatic upgrades for pre-production before beginning installation of the update.

For more information, see Upgrade clients in System Center Configuration Manager and How to test client upgrades in a pre-production collection in System Center Configuration Manager.

Plan to use service windows to control when site servers install updates:
Use service windows to define a period during which updates to a site server can be installed.

This can help you control when sites in your hierarchy install the update. For more information, see Service windows for site servers.

Review supported extensions:

If you extend Configuration Manager with other products from Microsoft or Microsoft partners, confirm that those products support version 1802. Check with the product vendor for this information. For example, see the Microsoft Deployment Toolkit release notes.

Run the setup prerequisite checker:
When the update is listed in the console as **Available,** you can independently run the prerequisite checker before installing the update. (When you install the update on the site, prerequisite checker runs again.)

To run a prerequisite check from the console, go to the **Administration** workspace, and select **Updates and Servicing**. Select the **Configuration Manager 1802** update package, and click **Run prerequisite check** in the ribbon.

For more information about starting and then monitoring the prerequisite check, see **Step 3: Run the prerequisite checker before installing an update** in the topic Install in-console updates for System Center Configuration Manager.

> **IMPORTANT**
> When the prerequisite checker runs independently or as part of an update installation, the process updates some product source files that are used for site maintenance tasks. Therefore, after running the prerequisite checker but before installing the update, if you need to perform a site maintenance task, run **Setupwpf.exe** (Configuration Manager Setup) from the CD.Latest folder on the site server.

Update sites:
You are now ready to start the update installation for your hierarchy. For more information about installing the update, see Install in-console updates..

We recommend that you plan to install the update outside of normal business hours for each site when the process of installing the update and its actions to reinstall site components and site system roles will have the least effect on your business operations.

For more information, see Updates for System Center Configuration Manager.

Post update Checklist

Review the following actions to take after the update installation is finished.

1. Make sure that site-to-site replication is active. In the console, view **Monitoring** > **Site Hierarchy**, and **Monitoring** > **Database Replication** for indications of problems or confirmation that replication links are active.

2. Make sure each site server and site system role has updated to version 1802. In the console, you can add the optional column **Version** to the display of some nodes including **Sites** and **Distribution Points**.

   When necessary, a site system role will reinstall automatically to update to the new version. Consider restarting remote site systems that do not update successfully.

3. Reconfigure database replicas for management points at primary sites that you disabled before starting the update.

4. Reconfigure database maintenance tasks that you disabled before starting the update.

5. If you configured client piloting before installing the update, upgrade clients per the plan you created.

6. If you use any extensions to Configuration Manager, update them to the latest version to support this Configuration Manager update.

Support for Configuration Manager current branch versions

7/26/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Microsoft plans to release updates for Configuration Manager current branch a few times per year. For versions of Configuration Manager released prior to 1710, support is for 12 months. Beginning with version 1710, each update version remains in support for 18 months from its general availability release date. Microsoft provides technical support for the entire period of support. There are two distinct servicing phases that depend on the availability of the latest current branch version.

- **Security and Critical Updates** servicing phase - When running the latest current branch version of Configuration Manager, you receive both Security and Critical Updates.
- **Security Updates (Only)** servicing phase - After the release of a new current branch version, Microsoft only supports security updates to older versions for the remainder of that version's support lifecycle (shown in Figure 1).

(View graphic at full size)

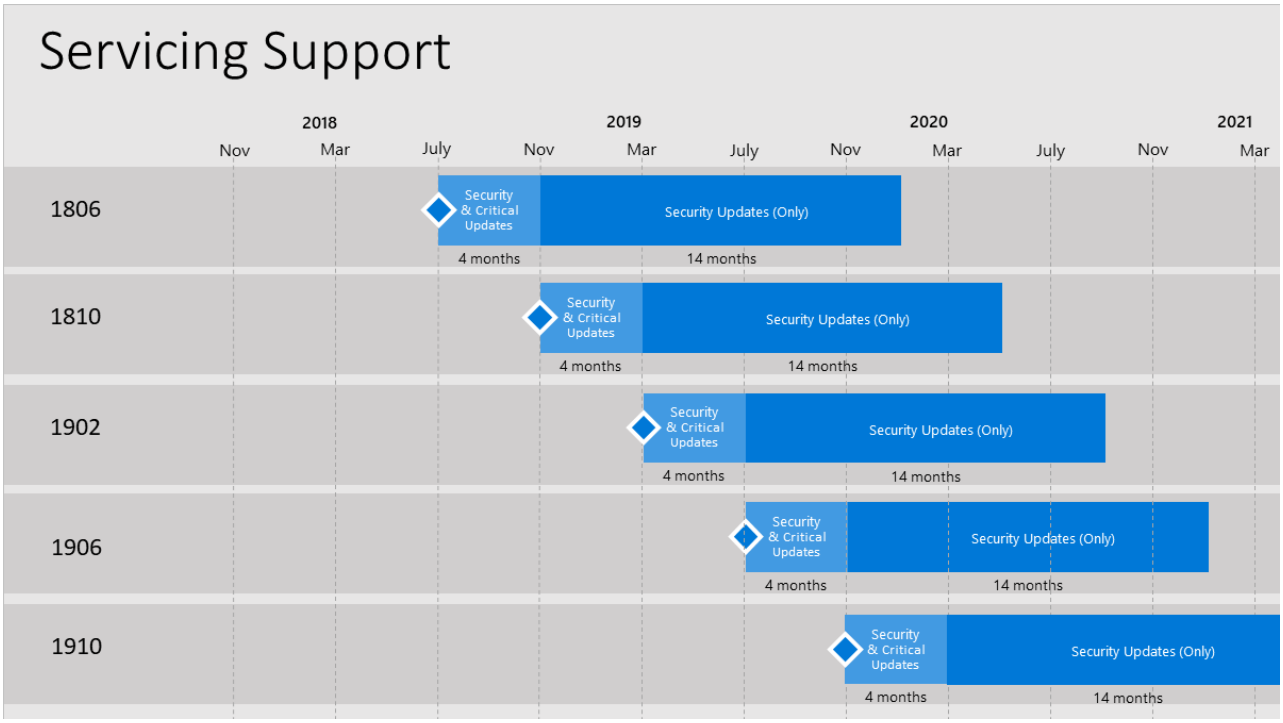


Figure 1. Example of the release cycle overlap for current branch servicing support. This example is for illustration of the cycle, and doesn't represent actual or expected release dates.

> **NOTE**
>
> The latest current branch version is always in the **Security and Critical Updates** servicing phase. This support statement means that if you encounter a code defect that warrants a critical update, you must have the latest current branch version installed in order to receive a fix. All other supported current branch versions are eligible to receive only security updates.
>
> All support ends after the 18-month lifecycle has expired for a current branch version.
>
> Update your Configuration Manager environment to the latest version before support for your current version expires.

For a list of the current branch versions, see Version details.

For more information about version numbers, and availability as an in-console update or as a baseline, see Baseline and update versions.

Back up a Configuration Manager site

7/9/2019 • 15 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Prepare backup and recovery approaches to avoid data loss. For Configuration Manager sites, a backup and recovery approach can help you to recover sites and hierarchies more quickly, and with the least data loss.

The sections in this article can help you back up your sites. To recover a site, see Recovery for Configuration Manager.

Considerations before creating a backup

- If you use a SQL Server Always On availability group to host the site database: Modify your backup and recovery plans as described in Prepare to use SQL Server Always On.
- Configuration Manager can recover the site database from the Configuration Manager backup task. It can also use a backup of the site database that you create with another process.

  For example, you can restore the site database from a backup that's created as part of a Microsoft SQL Server maintenance plan. You can also use a backup that's created by using Data Protection Manager to back up your site database.
- Starting with version 1806, install an additional site server in *passive* mode. The site server in passive mode is in addition to your existing site server in *active* mode. A site server in passive mode is available for immediate use, when needed. For more information, see Site server high availability. While this role doesn't remove the need to plan for and practice backup and recovery operations, it significantly reduces the effort to recover a site when necessary.

Using Data Protection Manager to back up your site database

You can use System Center Data Protection Manager (DPM) to back up your Configuration Manager site database.

Create a new protection group in DPM for the site database computer. On the **Select Group Members** page of the Create New Protection Group Wizard, you select the SMS Writer service from the data source list. Then select the site database as an appropriate member. For more information about using DPM, see the Data Protection Manager documentation library.

> **IMPORTANT**
> Configuration Manager doesn't support DPM backup for a SQL Server cluster that uses a named instance. It does support DPM backup on a SQL Server cluster that uses the default instance of SQL Server.

After you restore the site database, follow the steps in setup to recover the site. To use the site database that you backed up with Data Protection Manager, select the recovery option to **Use a site database that has been manually recovered**.

Backup maintenance task

You can automate backup for Configuration Manager sites by scheduling the predefined Backup Site Server maintenance task. This task has the following features:

- Runs on a schedule

- Backs up the site database
- Backs up specific registry keys
- Backs up specific folders and files
- Backs up the CD.Latest folder

Plan to run the default site backup task at a minimum of every five days. This schedule is because Configuration Manager uses a *SQL Server change tracking retention period* of five days. For more information, see SQL Server change tracking retention period.

To simplify the backup process, you can create an **AfterBackup.bat** file. This script automatically runs post-backup actions after the backup task completes successfully. Use the AfterBackup.bat file to archive the backup snapshot to a secure location. You can also use the AfterBackup.bat file to copy files to your backup folder, or to start other backup tasks.

You can back up a central administration site and primary site. Secondary sites or site system servers don't have backup tasks.

When the Configuration Manager backup service runs, it follows the instructions defined in the backup control file: `<ConfigMgrInstallationFolder>\Inboxes\Smsbkup.box\Smsbkup.ctl`. You can modify the backup control file to change the behavior of the backup service.

> **NOTE**
> Modifications of **Smsbkup.ctl** will apply after a restart of the service SMS_SITE_VSS_WRITER on the Site Server.

Site backup status information is written to the **Smsbkup.log** file. This file is created in the destination folder that you specify in the properties of the Backup Site Server maintenance task.

To enable the site backup maintenance task

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. Select the site for which you want to enable the site backup maintenance task.
3. Click **Site Maintenance Tasks** in the ribbon.
4. Select the **Backup Site Server** task, and click **Edit**.
5. Select the option to **Enable this task**. Click **Set Paths** to specify the backup destination. You have the following options:

   > **IMPORTANT**
   > To help prevent tampering of the backup files, store the files in a secure location. The most secure backup path is to a local drive, so you can set NTFS file permissions on the folder. Configuration Manager doesn't encrypt the backup data that's stored in the backup path.

   - **Local drive on site server for site data and database**: Specifies that the task stores the backup files for the site and site database in the specified path on the local disk drive of the site server. Create the local folder before the backup task runs. The Local System account on the site server must have **Write** NTFS file permissions to the local folder for the site server backup. The Local System account on the computer that's running SQL Server must have **Write** NTFS permissions to the folder for the site database backup.
   - **Network path (UNC name) for site data and database**: Specifies that the task stores the backup files for the site and site database in the specified network path. Create the share before the backup

task runs. The computer account of the site server must have **Write** NTFS and share permissions to the shared network folder. If SQL Server is installed on another computer, the computer account of the SQL Server must have the same permissions.

- **Local drives on site server and SQL Server**: Specifies that the task stores the backup files for the site in the specified path on the local drive of the site server. The task stores the backup files for the site database in the specified path on the local drive of the site database server. Create the local folders before the backup task runs. The computer account of the site server must have **Write** NTFS permissions to the folder that you create on the site server. The computer account of the SQL Server must have **Write** NTFS permissions to the folder that you create on the site database server. This option is available only when the site database isn't installed on the site server.

> **NOTE**
>
> The option to browse to the backup destination is only available when you specify the network path of the backup destination.
>
> The folder name or share name that's used for the backup destination doesn't support the use of Unicode characters.

6. Configure a schedule for the site backup task. Consider a backup schedule that's outside active working hours. If you have a hierarchy, consider a schedule that runs at least two times a week. If the site fails, this schedule ensures maximum data retention.

   When you run the Configuration Manager console on the same site server that you're configuring for backup, the backup task uses local time for the schedule. When you run the Configuration Manager console from another computer, the backup task uses Coordinated Universal Time (UTC) for the schedule.

7. Choose whether to create an alert if the site backup task fails. When selected, Configuration Manager creates a critical alert for the backup failure. You can review these alerts in the **Alerts** node of the **Monitoring** workspace.

Verify that the Backup Site Server maintenance task is running

- Check the timestamp on the files in the backup destination folder that the task created. Verify that the timestamp updates to the time when the task was last scheduled to run.
- Go to the **Component Status** node of the **Monitoring** workspace. Review the status messages for **SMS_SITE_BACKUP**. When site backup completes successfully, you see message ID **5035**. This message indicates that the site backup completed without any errors.
- When you configure the backup task to create an alert when it fails, look for backup failure alerts in the **Alerts** node of the **Monitoring** workspace.
- Open Windows Explorer on the site server and browse to `<ConfigMgrInstallationFolder>\Logs`. Review **Smsbkup.log** for warnings and errors. When site backup completes successfully, the log shows `Backup completed` with message ID `STATMSG: ID=5035`.

> **TIP**
>
> When the backup maintenance task fails, restart the backup task by stopping and restarting the **SMS_SITE_BACKUP** Windows service.

Archive the backup snapshot

The backup task creates a backup snapshot the first time it runs. You can use this snapshot to recover your site server if it fails. When the backup task runs again on schedule, it creates a new backup snapshot that overwrites the

previous snapshot. As a result, the site has only a single backup snapshot, and you've no way of retrieving an earlier backup snapshot.

Keep multiple archives of the backup snapshot for the following reasons:

- It's common for backup media to fail, get misplaced, or include only a partial backup. Recovering a failed stand-alone primary site from an older backup is better than recovering without any backup. For a site server in a hierarchy, the backup must be in the SQL Server change tracking retention period, or the backup isn't required.
- A corruption in the site can go undetected for several backup cycles. You might have to use a backup snapshot from before the site became corrupted. This reason applies to a stand-alone primary site and to sites in a hierarchy where the backup is in the SQL Server change tracking retention period.
- The site might have no backup snapshot at all. For example, if the Backup Site Server maintenance task fails. Because the backup task removes the previous backup snapshot before it starts to back up the current data, there won't be a valid backup snapshot.

Using the AfterBackup.bat file

After successfully backing up the site, the backup task automatically tries to run a script named **AfterBackup.bat**. Manually create the AfterBackup.bat file on the site server in `<ConfigMgrInstallationFolder>\Inboxes\Smsbkup.box`. If an AfterBackup.bat file exists in the correct folder, it automatically runs after the backup task completes.

The AfterBackup.bat file lets you archive the backup snapshot at the end of every backup operation. It can automatically perform other post-backup tasks that aren't part of the Backup Site Server maintenance task. The AfterBackup.bat file integrates the archive and the backup operations, thereby ensuring that every new backup snapshot is archived.

If the AfterBackup.bat file isn't present, the backup task skips it without effect on the backup operation. To verify that the backup task successfully ran this script, go to the **Component Status** node in the **Monitoring** workspace, and review the status messages for **SMS_SITE_BACKUP**. When the task successfully starts the AfterBackup.bat command file, you see message ID **5040**.

> **TIP**
> To archive your site server backup files with AfterBackup.bat, you must use a copy command tool in the batch file. One such tool is Robocopy in Windows Server. For example, create the AfterBackup.bat file with the following command:
> `Robocopy E:\ConfigMgr_Backup \\ServerName\ShareName\ConfigMgr_Backup /MIR`

Although the intended use of the AfterBackup.bat is to archive backup snapshots, you can create an AfterBackup.bat file to run additional tasks at the end of every backup operation.

Supplemental backup tasks

The Backup Site Server maintenance task provides a backup snapshot for the site server files and site database. There are other items not backed up that you must consider when you create your backup strategy. Use these sections to help you complete your Configuration Manager backup strategy.

Back up custom reports

If you modify predefined or created custom reports in SQL Server Reporting Services, create a backup for the report server database files. The report server backup must include the following components:

- The source files for reports and models
- Encryption keys

- Custom assemblies or extensions
- Configuration files
- Custom SQL Server views used in custom reports
- Custom stored procedures

> **IMPORTANT**
> When Configuration Manager updates to a newer version, the predefined reports might be overwritten by new reports. If you modify a predefined report, make sure to back up the report and then restore it in Reporting Services.

For more information about backing up your custom reports in Reporting Services, see Backup and Restore Operations for Reporting Services.

Back up content files

The content library in Configuration Manager is the location where all content files are stored for all software deployments. The content library is located on the site server and on each distribution point. The Backup Site Server maintenance task doesn't back up the content library or package source files. When a site server fails, the information about the content library is restored to the site database, but you must restore the content library and package source files.

- The content library must be restored before you can redistribute content to distribution points. When you start content redistribution, Configuration Manager copies the files from the site server's content library to the distribution points. For more information, see The content library.
- The package source files must be restored before you can update content on distribution points. When you start a content update, Configuration Manager copies new or modified files from the package source to the content library. It then copies the files to associated distribution points. Run the following SQL Server query against the site database to find the package source location for all packages and applications: `SELECT * FROM v_Package`. You can identify the package source site by looking at the first three characters of the package ID. For example, if the package ID is CEN00001, the site code for the source site is CEN. When you restore the package source files, they must be restored to the same location where they were before the failure.

Verify that you include both the content library and package source files in your file system backup for the site server.

Back up custom software updates

System Center Updates Publisher is a stand-alone tool that lets you manage custom software updates. Updates Publisher uses a local database for its software update repository. When you use Updates Publisher to manage custom software updates, determine whether you should include the Updates Publisher database in your backup plan. For more information, see System Center Updates Publisher.

Use the following procedure to back up the Updates Publisher database.

Back up the Updates Publisher database

1. On the computer that runs Updates Publisher, browse to the Updates Publisher database file **Scupdb.sdf** in `%USERPROFILE%\AppData\Local\Microsoft\System Center Updates Publisher 2011\5.00.1727.0000\`. There's a different database file for each user that runs Updates Publisher.
2. Copy the database file to your backup destination. For example, if your backup destination is `E:\ConfigMgr_Backup`, you could copy the Updates Publisher database file to `E:\ConfigMgr_Backup\SCUP`.

> **TIP**
> When there's more than one database file on a computer, consider storing the file in a subfolder that indicates the user profile associated with the database file. For example, you could have one database file in `E:\ConfigMgr_Backup\SCUP\User1` and another database file in `E:\ConfigMgr_Backup\SCUP\User2`.

User state migration data

You can use Configuration Manager task sequences to capture and restore the user state data in OS deployment scenarios. The properties of the state migration point list the folders that store the user state data. This data isn't backed up as part of the Site Server Backup maintenance task. As part of your backup plan, you must manually back up the folders that you specify to store the user state migration data.

Determine the folders used to store user state migration data

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Servers and Site System Roles** node.
2. Select the site system that hosts the state migration role. Then select **State migration point** in the **Site System Roles** pane.
3. Click **Properties** in the ribbon.
4. The folders that store the user state migration data are listed in the **Folder details** section on the **General** tab.

About the SMS Writer service

The SMS Writer is a service that interacts with the Windows Volume Shadow Copy Service (VSS) during the backup process. The SMS Writer service must be running for the Configuration Manager site back up to complete successfully.

Process

1. SMS Writer registers with the VSS service and binds to its interfaces and events.
2. When VSS broadcasts events, or if it sends specific notifications to the SMS Writer, the SMS Writer responds to the notification and takes the appropriate action.
3. The SMS Writer reads the backup control file **smsbkup.ctl** located in `<ConfigMgrInstallationPath>\inboxes\smsbkup.box`, and determines the files and data to back up.
4. The SMS Writer builds metadata, which consists of various components including specific data from the SMS registry key and subkeys. a. It sends the metadata to VSS when it's requested. b. VSS then sends the metadata to the requesting application, the Configuration Manager Backup Manager.
5. Backup Manager selects the data to back up, and sends this data to the SMS Writer via VSS.
6. The SMS Writer takes the appropriate steps to prepare for the backup.
7. Later, when VSS is ready to take the snapshot: a. It sends an event b. The SMS Writer stops all Configuration Manager services c. It ensures that the Configuration Manager activities are frozen while the snapshot is created.
8. After the snapshot is complete, the SMS Writer restarts services and activities.

The SMS Writer service is installed automatically. It must be running when the VSS application requests a backup or restore.

Writer ID

The writer ID for the SMS Writer is **03ba67dd-dc6d-4729-a038-251f7018463b**.

Permissions

The SMS Writer service must run under the Local System account.

Volume Shadow Copy service

The VSS is a set of COM APIs that implements a framework to allow volume backups to be performed while applications on a system continue to write to the volumes. The VSS provides a consistent interface that allows coordination between user applications that update data on disk (the SMS Writer service) and those that back up applications (the Backup Manager service). For more information, see the Volume Shadow Copy Service.

Next steps

After you create a backup, practice site recovery with that backup. This practice can help you become familiar with the recovery process before you need to rely on it. It can also help confirm the backup was successful for its intended purpose.

Recover a Configuration Manager site

8/26/2019 • 20 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Run a Configuration Manager site recovery after a site fails or data loss occurs in the site database. Repairing and resynchronizing data are the core tasks of a site recovery and are required to prevent interruption of operations.

The sections in this article can help you recover a Configuration Manager site. To create a backup, see Backup for Configuration Manager.

Considerations before recovering a site

> **IMPORTANT**
> This information applies only to site recovery scenarios. When you're upgrading your on-premises infrastructure and not actively recovering a failed site, review the information in the following articles:
>
> - Upgrade on-premises infrastructure
> - Modify your infrastructure

Prepare the server hardware

Make sure existing configurations aren't present on the site server. Any previous configurations can cause conflicts during the site recovery process. Use one of the following options for the server hardware:

- Use a new server, that meets the general and recovery requirements.
- Format the disks, and reinstall the OS on the existing server. Make sure it meets the general and recovery requirements.
- Reuse an existing server that you've cleaned

Use one of the following procedures to clean an existing server:

Clean an existing server for site server recovery only

1. Delete SMS registry keys: `HKLM\Software\Microsoft\SMS`
2. Delete any registry entries starting with `SMS` from `HKLM\System\CurrentControlSet\Services`. For example:
   - SMS_DISCOVERY_DATA_MANAGER
   - SMS_EXECUTIVE
   - SMS_INBOX_MONITOR
   - SMS_INVENTORY_DATA_LOADER
   - SMS_LAN_SENDER
   - SMS_MP_FILE_DISPATCH_MANAGER
   - SMS_SCHEDULER
   - SMS_SITE_BACKUP
   - SMS_SITE_COMPONENT_MANAGER
   - SMS_SITE_SQL_BACKUP
   - SMS_SITE_VSS_WRITER
   - SMS_SOFTWARE_METERING_PROCESSOR
   - SMS_STATE_SYSTEM

- SMS_STATUS_MANAGER
- SMS_WSUS_SYNC_MANAGER
- SMSvcHost 3.0.0.0
- SMSvcHost 4.0.0.0

3. Uninstall the Configuration Manager console
4. Restart the server
5. Confirm that all of the above registry keys are deleted.

The server is now ready for the Configuration Manager restore procedure.

Clean an existing server for site database recovery only

1. Back up the site database. Also back up any other supporting databases, like WSUS.
2. Make sure to note the SQL server name and instance name
3. Manually delete the site database from the SQL Server
4. Restart the SQL Server

The server is now ready for the Configuration Manager restore procedure.

Clean an existing server for full recovery

1. Back up the site database. Also back up any other supporting databases, like WSUS.
2. Make a copy of the content library
3. Manually delete the site database from the SQL Server
4. Uninstall the Configuration Manager site
5. Manually delete the Configuration Manager installation folder, and any other Configuration Manager folders
6. Restart the server
7. Restore the content library and other databases like WSUS

The server is now ready for the Configuration Manager restore procedure.

Use a supported version and same edition of SQL Server

If possible, use the same version of SQL Server. However, it's supported to restore a database to a newer version.

Don't change the SQL Server edition. Restoring a site database from Standard edition to Enterprise edition isn't supported.

Additional SQL Server configuration requirements:

- SQL Server can't be set to **single-user mode**.
- Make sure the MDF and LDF files are valid. When you recover a site, there's no check for the state of the files.

SQL Server Always On availability groups

If you use SQL Server Always On availability groups to host the site database, modify your recovery plans as described in Prepare to use SQL Server Always On.

Database replicas

After you restore a site database that you configured for database replicas, reconfigure each replica. Before you can use the database replicas, recreate both the publications and subscriptions.

Determine your recovery options

There are two main areas to consider for Configuration Manager primary site server and central administration site (CAS) recovery: the **site server** and the **site database**. The following sections can help you select the best options for your recovery scenario.

> **NOTE**
> When Configuration Manager setup detects an existing site on the server, you can start a site recovery, but the recovery options for the site server are limited. For example, if you run Setup on an existing site server, when you choose recovery, you can recover the site database server, but the option to recover the site server is disabled.

Site server recovery options

Start Configuration Manager setup from a copy of the **CD.Latest** folder that you created outside of the Configuration Manager installation folder.

- If you run setup from the **Start** menu on the site server, the **Recover a site** option isn't available.
- If you installed any updates from within the Configuration Manager console before you made your backup, you can't reinstall the site by using setup from the following locations:
  - Installation media
  - The Configuration Manager installation path

Then select the **Recover a site** option. You have the following recovery options for the failed site server:

Recover the site server using an existing backup

Use this option when you have a Configuration Manager backup of the site server from before the site failure. The site creates this backup as part of the **Backup Site Server** maintenance task. The site is reinstalled, and the site settings are configured based on the site that was backed up.

Reinstall the site server

Use this option when you don't have a backup of the site server. The site server is reinstalled, and you must specify the site settings as you would during an initial installation.

- Use the same site code and site database name that you used when the failed site was first installed.
- You can reinstall the site on a new computer that runs a new OS version.
- The server must use the same hostname and fully qualified domain name (FQDN) of the original site server.

Site database recovery options

When you run Configuration Manager setup, you have the following recovery options for the site database:

Recover the site database using a backup set

Use this option when you have a Configuration Manager backup of the site database from before the database failure. The site creates this backup as part of the **Backup Site Server** maintenance task. In a hierarchy, when restoring a primary site, the recovery process retrieves from the CAS any changes made to the site database after the last backup. When restoring the CAS, the recovery process retrieves these changes from a reference primary site. When you recover the site database for a standalone primary site, you lose site changes after the last backup.

When you recover the site database for a site in a hierarchy, the recovery behavior is different for a CAS and primary site. The behavior is also different when the last backup is inside or outside of the SQL Server change tracking retention period. For more information, see the Site database recovery scenarios section in this article.

> **NOTE**
> If you select to restore the site database by using a backup set, but the site database already exists, the recovery fails.

Create a new database for this site

Use this option when you don't have a backup of the site database. In a hierarchy, the recovery process creates a new site database. When restoring a child primary site, it recovers the data by replicating from the CAS. When restoring the CAS, it replicates data from a reference primary site. This option isn't available when you're

recovering a standalone primary site or a CAS that doesn't have primary sites.

Use a site database that has been manually recovered

Use this option when you've already recovered the Configuration Manager site database, but need to complete the recovery process.

- Configuration Manager can recover the site database from any of the following processes:
  - The Configuration Manager backup maintenance task
  - A site database backup using Data Protection Manager (DPM)
  - Another backup process

    After you restore the site database by using a method outside Configuration Manager, run Setup, and select this option to complete the site database recovery.

    > **NOTE**
    > When you use DPM to back up your site database, use the DPM procedures to restore the site database to a specified location before you continue the restore process in Configuration Manager. For more information about DPM, see the Data Protection Manager documentation library.

- In a hierarchy, when you recover a primary site database, the recovery process retrieves from the CAS any changes made to the site database after the last backup. When restoring the CAS, the recovery process retrieves these changes from a reference primary site. When you recover the site database for a standalone primary site, you lose site changes after the last backup.

Skip database recovery

Use this option when no data loss has occurred on the Configuration Manager site database server. This option is only valid when the site database is on a different computer than the site server that you're recovering.

SQL Server change tracking retention period

Configuration Manager enables change tracking for the site database in SQL Server. Change tracking lets Configuration Manager query for information about the changes made to database tables after a previous point in time. The retention period specifies how long change tracking information is kept. By default, the site database is configured to have a retention period of five days. When you recover a site database, the recovery process proceeds differently if your backup is inside or outside the retention period. For example, if your SQL server fails, and your last backup is seven days old, it's outside the retention period.

For more information about SQL Server change tracking internals, see the following blog posts from the SQL Server team: Change Tracking Cleanup - part 1 and Change Tracking Cleanup - part 2.

Reinitialization of site or global data

The process to reinitialize site or global data replaces existing data in the site database with data from another site database. For example, when site ABC reinitializes data from site XYZ, the following steps occur:

- The data is copied from site XYZ to site ABC.
- The existing data for site XYZ is removed from the site database on site ABC.
- The copied data from site XYZ is inserted into the site database for site ABC.

Example scenario 1: The primary site reinitializes the global data from the CAS

The recovery process removes the existing global data for the primary site in the primary site database and replaces the data with the global data copied from the CAS.

Example scenario 2: The CAS reinitializes the site data from a primary site

The recovery process removes the existing site data for that primary site in the CAS database. It replaces the data

with the site data copied from the primary site. The site data for other primary sites isn't affected.

Site database recovery scenarios

After a site database is restored from a backup, Configuration Manager tries to restore the changes in site and global data after the last database backup. Configuration Manager starts the following actions after a site database is restored from backup:

Recovered site is a CAS

- Database backup within change tracking retention period
  - **Global data**: The changes in global data after the backup are replicated from all primary sites.
  - **Site data**: The changes in site data after the backup are replicated from all primary sites.
- Database backup older than change tracking retention period
  - **Global data**: The CAS reinitializes the global data from the reference primary site if you specify it. Then all other primary sites reinitialize the global data from the CAS. If you don't specify a reference site, all primary sites reinitialize the global data from the CAS. This data is what you restored from backup.
  - **Site data**: The CAS reinitializes the site data from each primary site.

Recovered site is a primary site

- Database backup within change tracking retention period
  - **Global data**: The changes in global data after the backup are replicated from the CAS.
  - **Site data**: The CAS reinitializes the site data from the primary site. Changes after the backup are lost. Clients regenerate most data when they send information to the primary site.
- Database backup older than change tracking retention period
  - **Global data**: The primary site reinitializes the global data from the CAS.
  - **Site data**: The CAS reinitializes the site data from the primary site. Changes after the backup are lost. Clients regenerate most data when they send information to the primary site.

Site recovery procedures

Use one of the following procedures to help you recover your site server and site database:

Start a site recovery in the setup wizard

1. Copy the CD.Latest folder to a location outside the Configuration Manager installation folder. From the copy of the CD.Latest folder, run the Configuration Manager setup wizard.
2. On the **Getting Started** page, select **Recover a site**, and then select **Next**.
3. Complete the wizard by using the options that are appropriate for your site recovery.
   - During the recovery, setup identifies the SQL Server Service Broker (SSB) port used by the SQL Server. Don't change this port setting during recovery or data replication won't work properly after the recovery completes.
   - You can specify the original or a new path to use for the Configuration Manager installation in the setup wizard.

Start an unattended site recovery

1. Prepare the unattended installation script for the options that you require for the site recovery. For more information, see Unattended site recovery.

2. Run Configuration Manager setup by using the `/script` command-line option. For example, you create a setup initialization file **ConfigMgrUnattend.ini**. You save it in the `C:\Temp` directory of the computer on which you're running setup. Use the following command:

   ```
   setup.exe /script C:\temp\ConfigMgrUnattend.ini
   ```

> **NOTE**
>
> After you recover a CAS, replication of some site data from child sites can fail to be established. This data can include hardware inventory, software inventory, and status messages.
>
> If this issue occurs, reinitialize the **ConfigMgrDRSSiteQueue** for database replication. Use **SQL Server Manager** to run the following query against the site database for the CAS:
>
> ```
> IF EXISTS (SELECT * FROM sys.service_queues WHERE name = 'ConfigMgrDRSSiteQueue' AND is_receive_enabled =
> 0)
>
> ALTER QUEUE [dbo].[ConfigMgrDRSSiteQueue] WITH STATUS = ON
> ```

Post-recovery tasks

After you recover your site, there are several post-recovery tasks to consider before your site recovery is complete. Use the following sections to help you complete your site recovery process.

Reenter user account passwords

After a site server recovery, reenter the passwords for any user accounts in the site. These passwords are reset during the site recovery. The accounts are listed on the **Finished** page of the setup wizard after site recovery is completed. The list is also saved to `C:\ConfigMgrPostRecoveryActions.html` on the recovered site server.

Reenter user account passwords after site recovery

1. Open the Configuration Manager console and connect to the recovered site.
2. Go to the **Administration** workspace, expand **Security**, and then select **Accounts**.
3. For each account, do the following steps to reenter the password:
   a. Select the account from the list identified after site recovery.
   b. Select **Properties** in the ribbon.
   c. On the **General** tab, select **Set**, and then reenter the password for the account.
   d. Select **Verify**, choose the appropriate data source for the selected user account, and then select **Test connection**. This step tests that the user account can connect to the data source, and verifies the credentials.
   e. Select **OK** to save the password changes, and then select **OK** to close the account properties page.

Reenter PXE passwords

1. In the Configuration Manager console, go to the **Administration** workspace, and select the **Distribution Points** node. Any on-premises distribution point with **Yes** in the **PXE** column is enabled for PXE and may have a password to reenter.
2. Select a PXE-enabled distribution point, and select **Properties** in the ribbon.
3. Switch to the **PXE** tab.
4. If the option to **Require a password when computers use PXE** is enabled, enter and confirm the password.

5. Select **OK** to save and close the properties.

Repeat this process for any other PXE-enabled on-premises distribution point.

Reenter task sequence passwords

1. In the Configuration Manager console, go to the **Software Library** workspace, expand **Operating Systems**, and select the **Task Sequences** node.
2. Select a task sequence, and then in the ribbon, select **Edit**.
3. Review the following steps for passwords to reenter:
   - **Apply Windows Settings**: If you enable and specify the local administrator password, reenter and confirm the password.
   - **Apply Network Settings**: For the account that has permission to join the domain, select **Set**. Enter and confirm the password, and then select **Verify**.
   - **Capture Operating System Image**: For the account used to access the destination, select **Set**. Enter and confirm the password, and then select **Verify**.
   - **Connect to Network Folder**: For the account used to connect a network folder, select **Set**. Enter and confirm the password, and then select **Verify**.
   - **Enable BitLocker**: If you use the key management option **TPM and PIN**, reenter the PIN.
   - **Join Domain or Workgroup**: For the account that has permission to join the domain, select **Set**. Enter and confirm the password, and then select **Verify**.
   - **Run Command Line**: If you use the option to **Run this step as the following account**, select **Set**. Enter and confirm the password, and then select **Verify**.
   - **Run PowerShell Script**: If you use the option to **Run this step as the following account**, select **Set**. Enter and confirm the password, and then select **Verify**.

Repeat this process for all task sequences.

Reenter sideloading keys

After a site server recovery, reenter Windows sideloading keys specified for the site. These keys are reset during site recovery. After you reenter the sideloading keys, the site resets the count in the **Activations used** column for Windows sideloading keys.

For example, before the site failure the **Total activations** count shows as **100**. The number of keys that devices have used, or **Activations used**, is **90**. After the site recovery, the **Total activations** value still displays **100**, but the **Activations used** column incorrectly displays **0**. After 10 new devices use a sideloading key, there are no more sideloading keys, and the 11th device fails to apply a sideloading key.

Recreate the Microsoft Intune subscription

If you recover a Configuration Manager site server after the site server is reimaged, the Microsoft Intune subscription isn't restored. Reconnect your subscription after you recover the site. Don't create a new APN request. Instead upload the current valid PEM file. Use the same file that you uploaded the last time you configured or renewed iOS management. For more information, see Configuring the Microsoft Intune subscription.

Recreate Azure services

In Configuration Manager version 1806, after site recovery you'll see the following error in the cloudmgr.log:

```
Index (zero-based) must be greater than or equal to zero
```

To resolve this, Renew the secret key for each Azure tenant connection.

Configure SSL for site system roles that use IIS

When you recover site systems that run IIS and you configured for HTTPS, reconfigure IIS to use the web server certificate.

Reinstall hotfixes

After a site recovery, you must reinstall any out-of-band hotfixes that were applied to the site server. After site recovery, view the list of the previously installed hotfixes on the **Finished** page of the setup wizard. This list is also saved to `C:\ConfigMgrPostRecoveryActions.html` on the recovered site server.

Recover custom reports

Some customers create custom reports in SQL Server Reporting Services. When this component fails, recover the reports from a backup of the report server. For more information about restoring your custom reports in Reporting Services, see Backup and Restore Operations for Reporting Services.

Recover content files

The site database tracks where the site server stores the content files. The content files themselves aren't backed up or restored as part of the backup and recovery process. To fully recover content files, restore the content library and package source files to the original location. There are several methods for recovering your content files. The easiest method is to restore the files from a file system backup of the site server.

If you don't have a file system backup for the package source files, manually copy or download them. This process is similar to when you originally created the package. Run the following query in SQL Server to find the package source location for all packages and applications: `SELECT * FROM v_Package`. Identify the package source site by looking at the first three characters of the package ID. For example, if the package ID is CEN00001, the site code for the source site is CEN. When you restore the package source files, they must be restored to the same location in which they were before the failure.

If you don't have a file system backup that includes the content library, you have the following restore options:

- **Import a prestaged content file**: In a Configuration Manager hierarchy, you can create a prestaged content file with all packages and applications from another location. Then import the prestaged content file to recover the content library on the site server.
- **Update content**: Configuration Manager copies the content from the package source to the content library. For this action to finish successfully, the package source files must be available in the original location. Do this action on each package and application.

Recover custom software updates

When you've included System Center Updates Publisher database files in your backup plan, you can recover the databases if the Updates Publisher computer fails. For more information about Updates Publisher, see System Center Updates Publisher.

Restore the Updates Publisher database

1. Reinstall Updates Publisher on the recovered computer.
2. Copy the database file **Scupdb.sdf** from your backup destination to `%USERPROFILE%\AppData\Local\Microsoft\System Center Updates Publisher 2011\5.00.1727.0000\` on the computer that runs Updates Publisher.
3. When more than one user runs Updates Publisher on the computer, copy each database file to the appropriate user profile location.

User State Migration data

As part of the state migration point properties, you specify the folders that store user state data. After you recover a state migration point, manually restore the user state data on the server. Restore it to the same folders that stored the data before the failure.

Regenerate the certificates for distribution points

After you restore a site, the **distmgr.log** might list the following entry for one or more distribution points: `Failed to decrypt cert PFX data`. This entry indicates that the distribution point certificate data can't be decrypted by the site. To resolve this issue, regenerate or reimport the certificate for affected distribution points. Use the Set-CMDistributionPoint PowerShell cmdlet.

Update certificates used for cloud-based distribution points

Configuration Manager requires an Azure management certificate for the site server to communicate with cloud-based distribution points. After a site recovery, update the certificates for cloud-based distribution points.

Recover a secondary site

Configuration Manager doesn't support the backup of the database at a secondary site, but does support recovery by reinstalling the secondary site. Secondary site recovery is required when a Configuration Manager secondary site fails.

Requirements

- The server must meet all secondary site prerequisites and have appropriate security rights configured.
- Use the same installation path that was used for the failed site.
- Use a server with the same configuration as the failed server. This configuration includes its fully qualified domain name (FQDN).
- The server must have the same SQL Server configuration as the failed site.
  - During a secondary site recovery, Configuration Manager doesn't install SQL Server Express if it's not already installed on the computer.
  - Use the same version of SQL Server and the same instance of SQL Server that you used for the secondary site database before the failure.

Procedure

Use the **Recover Secondary Site** action from the **Sites** node in the Configuration Manager console. Unlike with other types of sites, recovery for a secondary site doesn't use a backup file. This process reinstalls the secondary site files on the failed server. After the site reinstalls, the secondary site data is reinitialized from the parent primary site.

During the recovery process, Configuration Manager verifies if the content library exists on the secondary site server. It also checks that the appropriate content is available. The secondary site uses the existing content library, if it includes the appropriate content. Otherwise, to recover the content library of a secondary site, redistribute or prestage the content to the server.

When you have a distribution point that isn't on the secondary site server, you aren't required to reinstall the distribution point during a recovery of the secondary site. After the secondary site recovery, the site automatically synchronizes with the distribution point.

You can verify the status of the secondary site recovery by using the **Show Install Status** action from the **Sites** node in the Configuration Manager console.

Unattended site recovery for Configuration Manager

5/9/2019 • 12 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To perform an unattended recovery of a Configuration Manager central administration site or primary site, you can create an unattended installation script and then use setup with the **/script** command option. The script provides the same type of information that the setup wizard prompts for, except that there are no default settings. All values must be specified for the setup keys that apply to the type of recovery you are using.

To use the /script setup command-line option, you must create an initialization file. Then specify this file name after the /script option. The name of the file is unimportant as long as it has the **.ini** file name extension. When you reference the setup initialization file from the command line, you must provide the full path to the file. For example, if your setup initialization file is named *setup.ini*, and it is stored in the *C:\setup folder*, your command line would be:

```
setup /script c:\setup\setup.ini
```

> **IMPORTANT**
> You must have Administrator rights to run setup. When you run setup with the unattended script, start the command prompt in an Administrator context by using **Run as administrator**.

The script contains section names, key names, and values. Required section key names vary depending on the recovery type that you are scripting. The order of the keys within sections, and the order of sections within the file, is not important. The keys are not case-sensitive. When you provide values for keys, the name of the key must be followed by an equals sign (=) and the value for the key.

Use the following sections to help you to create your script for unattended site recovery. The tables list the available setup script keys, their corresponding values, whether they are required, which type of installation they are used for, and a short description for the key.

Recover a central administration site unattended

Use the following information to configure an unattended setup script file to recover a central administration site.

Identification

- **Key name:** Action
  - **Required:** Yes
  - **Values:** RecoverCCAR
  - **Details:** Recovers a central administration site
- **Key Name:** CDLatest
  - **Required:** Yes – Only when using media from the CD.Latest folder.
  - **Values:** 1 Any value other than 1 is considered to not be using CD.Latest.
  - **Details:** Your script must include this key and value when you run setup from media in a CD.Latest folder for the purpose of installing a primary or central administration site, or recovering a primary or central administration site. This value informs setup that media form CD.Latest is being used.

RecoveryOptions

- **Key name:** ServerRecoveryOptions
  - **Required:** Yes
  - **Values:** 1, 2, or 4
    1 = Recovery site server and SQL Server.
    2 = Recover site server only.
    4 = Recover SQL Server only.
  - **Details:** Specifies whether setup recovers the site server, SQL Server, or both. The associated keys are required when you set the following value for the ServerRecoveryOptions setting:
    - **Value = 1** You have the option to specify a value for the **SiteServerBackupLocation** key to recover the site by using a site backup. If you do not specify a value, the site is reinstalled without restoring it from a backup set.

      The **BackupLocation** key is required when you configure a value of **10** for the **DatabaseRecoveryOptions** key, which is to restore the site database from backup.
    - **Value = 2** You have the option to specify a value for the **SiteServerBackupLocation** key to recover the site by using a site backup. If you do not specify a value, the site is reinstalled without restoring it from a backup set.
    - **Value = 4** The **BackupLocation** key is required when you configure a value of **10** for the **DatabaseRecoveryOptions** key, which is to restore the site database from backup.
- **Key name:** DatabaseRecoveryOptions
  - **Required:** Maybe
  - **Values:**
    - **10** = Restore the site database from backup.
    - **20** = Use a site database that has been manually recovered by using another method.
    - **40** = Create a new database for the site. Use this option when there is no site database backup available. Global and site data is recovered through replication from other sites.
    - **80** = skip database recovery.
  - **Details:** Specifies how setup recovers the site database in SQL Server. This key is required when the **ServerRecoveryOptions** setting has a value of **1** or **4**.
- **Key name:** ReferenceSite
  - **Required:** Maybe
  - **Values:** <ReferenceSiteFQDN>
  - **Details:** Specifies the reference primary site. If the database backup is older than the change tracking retention period, or you recover the site without a backup, the central administration site uses the reference site to recover global data.

    When you do not specify a reference site, and the backup is older than the change tracking retention period, all primary sites are reinitialized with the restored data from the central administration site.

    When you do not specify a reference site, and the backup is within the change tracking retention period, only changes since the backup are replicated from primary sites. When there are conflicting changes from different primary sites, the central administration site uses the first one that it receives.

    This key is required when the **DatabaseRecoveryOptions** setting has a value of **40**.
- **Key name:** SiteServerBackupLocation
  - **Required:** No
  - **Values:** <PathToSiteServerBackupSet>

- **Details:** Specifies the path to the site server backup set. This key is optional when the **ServerRecoveryOptions** setting has a value of **1** or **2**. Specify a value for the **SiteServerBackupLocation** key to recover the site by using a site backup. If you do not specify a value, the site is reinstalled without restoring it from a backup set.

- **Key name:** BackupLocation
  - **Required:** Maybe
  - **Values:** <PathToSiteDatabaseBackupSet>
  - **Details:** Specifies the path to the site database backup set. The **BackupLocation** key is required when you configure a value of **1** or **4** for the **ServerRecoveryOptions** key, and configure a value of **10** for the **DatabaseRecoveryOptions** key.

Options

- **Key name:** ProductID
  - **Required:** Yes
  - **Values:**
    - xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
    - Eval
  - **Details:** The Configuration Manager installation product key, including the dashes. Enter **Eval** can install the evaluation version of Configuration Manager.
- **Key name:** SiteCode
  - **Required:** Yes
  - **Values:** <Site code>
  - **Details:** Three alpha-numeric characters that uniquely identify the site in your hierarchy. Specify the site code that was used by the site before the failure.
- **Key name:** SiteName
  - **Required:** Yes
  - **Values:** SiteName
  - **Details:** Description for this site.
- **Key name:** SMSInstallDir
  - **Required:** Yes
  - **Values:** <*ConfigMgrInstallationPath*>
  - **Details:** Specifies the installation folder for the Configuration Manager program files.

    > **NOTE**
    > You can specify the original path or a new path to use for the Configuration Manager installation.

- **Key name:** SDKServer
  - **Required:** Yes
  - **Values:** <*FQDN of SMS Provider*>
  - **Details:** Specifies the FQDN for the server that hosts the SMS Provider. Specify the server that hosted the SMS Provider before the failure.

    You can configure additional SMS Providers for the site after the initial installation.

- **Key name:** PrerequisiteComp

- **Required:** Yes
- **Values:** 0 or 1
  0 = download
  1 = already downloaded
- **Details:** Specifies whether setup prerequisite files have already been downloaded. For example, if you use a value of 0, setup downloads the files.

- **Key name:** PrerequisitePath
  - **Required:** Yes
  - **Values:** <*PathToSetupPrerequisiteFiles*>
  - **Details:** Specifies the path to the setup prerequisite files. Depending on the **PrerequisiteComp** value, setup uses this path to store downloaded files or to locate previously downloaded files.
- **Key name:** AdminConsole
  - **Required:** Maybe
  - **Values:** 0 or 1 0 = do not install
    1 = install
  - **Details:** Specifies whether to install the Configuration Manager console. This key is required except when the **ServerRecoveryOptions** setting has a value of **4**.
- **Key name:** JoinCEIP

  > **NOTE**
  > Starting in Configuration Manager version 1802 the CEIP feature is removed from the product.

  - **Required:** Yes
  - **Values:** 0 or 1
    0 = do not join
    1 = join
  - **Details:** Specifies whether to join the Customer Experience Improvement Program.

SQLConfigOptions

- **Key name:** SQLServerName
  - **Required:** Yes
  - **Values:** <*SQLServerName*>
  - **Details:** The name of the server, or clustered instance name, running SQL Server that hosts the site database. Specify the same server that hosted the site database before the failure.
- **Key name:** DatabaseName
  - **Required:** Yes
  - **Values:** <*SiteDatabaseName*> or <*InstanceName*>\<*SiteDatabaseName*>
  - **Details:** The name of the SQL Server database to create or use to install the central administration site database. Specify the same database name that was used before the failure.

    > **IMPORTANT**
    > If you do not use the default instance, you must specify the instance name and site database name.

- **Key name:** SQLSSBPort

- **Required:** No
- **Values:** <*SSBPortNumber*>
- **Details:** Specify the SQL Server Service Broker (SSB) port used by SQL Server. Typically, SSB is configured to use TCP port 4022, but other ports are supported. Specify the same SSB port that was used before the failure.

Recover a Primary Site Unattended

Use the following information to configure an unattended setup script file to recover a central administration site.

Identification

- **Key name:** Action
  - **Required:** Yes
  - **Values:** RecoverPrimarySite
  - **Details:** Recovers a primary site
- **Key Name:** CDLatest
  - **Required:** Yes – Only when using media from the CD.Latest folder.
  - **Values:** 1 Any value other than 1 is considered to not be using CD.Latest.
  - **Details:** Your script must include this key and value when you run setup from media in a CD.Latest folder for the purpose of installing a primary or central administration site, or recovering a primary or central administration site. This value informs setup that media form CD.Latest is being used.

RecoveryOptions

- **Key name:** ServerRecoveryOptions
  - **Required:** Yes
  - **Values:** 1, 2, or 4
    1 = Recovery site server and SQL Server.
    2 = Recover site server only.
    4 = Recover SQL Server only.
  - **Details:** Specifies whether setup recovers the site server, SQL Server, or both. The associated keys are required when you set the following value for the ServerRecoveryOptions setting:
    - **Value = 1** You have the option to specify a value for the **SiteServerBackupLocation** key to recover the site by using a site backup. If you do not specify a value, the site is reinstalled without restoring it from a backup set.

      The **BackupLocation** key is required when you configure a value of **10** for the **DatabaseRecoveryOptions** key, which is to restore the site database from backup.
    - **Value = 2** You have the option to specify a value for the **SiteServerBackupLocation** key to recover the site by using a site backup. If you do not specify a value, the site is reinstalled without restoring it from a backup set.
    - **Value = 4** The **BackupLocation** key is required when you configure a value of **10** for the **DatabaseRecoveryOptions** key, which is to restore the site database from backup.
- **Key name:** DatabaseRecoveryOptions
  - **Required:** Maybe
  - **Values:**
    - **10** = Restore the site database from backup.

    - **20** = Use a site database that has been manually recovered by using another method.
    - **40** = Create a new database for the site. Use this option when there is no site database backup available. Global and site data is recovered through replication from other sites.
    - **80** = skip database recovery.
  - **Details:** Specifies how setup recovers the site database in SQL Server. This key is required when the **ServerRecoveryOptions** setting has a value of **1** or **4**.
- **Key name:** SiteServerBackupLocation
  - **Required:** No
  - **Values:** <PathToSiteServerBackupSet>
  - **Details:** Specifies the path to the site server backup set. This key is optional when the **ServerRecoveryOptions** setting has a value of **1** or **2**. Specify a value for the **SiteServerBackupLocation** key to recover the site by using a site backup. If you do not specify a value, the site is reinstalled without restoring it from a backup set.
- **Key name:** BackupLocation
  - **Required:** Maybe
  - **Values:** <PathToSiteDatabaseBackupSet>
  - **Details:** Specifies the path to the site database backup set. The **BackupLocation** key is required when you configure a value of **1** or **4** for the **ServerRecoveryOptions** key, and configure a value of **10** for the **DatabaseRecoveryOptions** key.

Options

- **Key name:** ProductID
  - **Required:** Yes
  - **Values:**
    - xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
    - Eval
  - **Details:** The Configuration Manager installation product key, including the dashes. Enter **Eval** can install the evaluation version of Configuration Manager.
- **Key name:** SiteCode
  - **Required:** Yes
  - **Values:** <Site code>
  - **Details:** Three alpha-numeric characters that uniquely identify the site in your hierarchy. Specify the site code that was used by the site before the failure.
- **Key name:** SiteName
  - **Required:** Yes
  - **Values:** SiteName
  - **Details:** Description for this site.
- **Key name:** SMSInstallDir
  - **Required:** Yes
  - **Values:** <*ConfigMgrInstallationPath*>
  - **Details:** Specifies the installation folder for the Configuration Manager program files.

> **NOTE**
> You can specify the original path or a new path to use for the Configuration Manager installation.

- **Key name:** SDKServer
  - **Required:** Yes
  - **Values:** *<FQDN of SMS Provider>*
  - **Details:** Specifies the FQDN for the server that hosts the SMS Provider. Specify the server that hosted the SMS Provider before the failure.

    You can configure additional SMS Providers for the site after the initial installation.
- **Key name:** PrerequisiteComp
  - **Required:** Yes
  - **Values:** 0 or 1
    0 = download
    1 = already downloaded
  - **Details:** Specifies whether setup prerequisite files have already been downloaded. For example, if you use a value of 0, setup downloads the files.
- **Key name:** PrerequisitePath
  - **Required:** Yes
  - **Values:** *<PathToSetupPrerequisiteFiles>*
  - **Details:** Specifies the path to the setup prerequisite files. Depending on the **PrerequisiteComp** value, setup uses this path to store downloaded files or to locate previously downloaded files.
- **Key name:** AdminConsole
  - **Required:** Maybe
  - **Values:** 0 or 1
    0 = do not install
    1 = install
  - **Details:** Specifies whether to install the Configuration Manager console. This key is required except when the **ServerRecoveryOptions** setting has a value of **4**.
- **Key name:** JoinCEIP

  > **NOTE**
  > Starting in Configuration Manager version 1802 the CEIP feature is removed from the product.

  - **Required:** Yes
  - **Values:** 0 or 1
    0 = do not join
    1 = join
  - **Details:** Specifies whether to join the Customer Experience Improvement Program.

SQLConfigOptions

- **Key name:** SQLServerName
  - **Required:** Yes

- **Values:** <*SQLServerName*>
- **Details:** The name of the server, or clustered instance name, running SQL Server that hosts the site database. Specify the same server that hosted the site database before the failure.

- **Key name:** DatabaseName
  - **Required:** Yes
  - **Values:** <*SiteDatabaseName*> or <*InstanceName*>\<*SiteDatabaseName*>
  - **Details:** The name of the SQL Server database to create or use to install the central administration site database. Specify the same database name that was used before the failure.

    > **IMPORTANT**
    > If you do not use the default instance, you must specify the instance name and site database name.

- **Key name:** SQLSSBPort
  - **Required:** No
  - **Values:** <*SSBPortNumber*>
  - **Details:** Specify the SQL Server Service Broker (SSB) port used by SQL Server. Typically, SSB is configured to use TCP port 4022, but other ports are supported. Specify the same SSB port that was used before the failure.

Hierarchy ExpansionOption

- **Key name:** CCARSiteServer
  - **Required:** Maybe
  - **Values:** <*SiteCodeForCentralAdministrationSite*>
  - **Details:** Specifies the central administration site that a primary site attaches to when it joins the Configuration Manager hierarchy. This setting is required if the primary site was attached to a central administration site before the failure. Specify the site code that was used for the central administration site before the failure.
- **Key name:** CASRetryInterval
  - **Required:** No
  - **Values:** <*Interval*>
  - **Details:** Specifies the retry interval (in minutes) to attempt a connection to the central administration site after the connection fails. For example, if the connection to the central administration site fails, the primary site waits the number of minutes that you specify for CASRetryInterval, and then reattempts the connection.
- **Key name:** WaitForCASTimeout
  - **Required:** No
  - **Values:** <*Timeout*>
  - **Details:** Specifies the maximum timeout value (in minutes) for a primary site to connect to the central administration site. For example, if a primary site fails to connect to a central administration site, the primary site retries the connection to the central administration site based on the CASRetryInterval until the WaitForCASTimeout period is reached. You can specify a value of 0 to 100.

Site failure impacts in Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The site server and any of the other site systems can fail and cause a loss of the services they regularly provide. If you install multiple site systems on the same computer, and that computer fails, all services regularly provided by those site systems are no longer available.

Part of your planning process should include understanding the impact on the service that you provide your organization. Because each site system in the site provides different functionality, the impact of a failure on the site differs, depending on the role of the site system that failed.

Use high availability options to help mitigate the failure of any single system. Also plan for and practice a backup and recovery strategy to reduce the amount of time the service is unavailable.

The following sections describe the impact when the specified site system isn't operational:

Site server

- No site administration is possible. You can't connect the console to the site.
- The management point collects client information and caches it until the site server is back online.
- Users can run existing deployments, and clients can download content from distribution points.

Site database

- No site administration is possible.
- If the Configuration Manager client already has a policy assignment with new policies, and if the management point has cached the policy body, the client can make a policy body request and receive the policy body reply. However, the site can't service any new policy assignment requests.
- Clients can run deployments, only if they've already received the policy, and the associated source files are already cached locally at the client.

Management point

- Although you can create new deployments, clients don't receive them until a management point is online.
- Clients still collect inventory, software metering, and status information. They store this data locally until the management point is available.
- Clients can run deployments, only if they've already received the policy, and the associated source files are already cached locally at the client.

Distribution point

- Configuration Manager clients can run deployments, only if the associated source files have already been downloaded locally or are available on a peer source.

Monitor the hierarchy

8/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To monitor your hierarchy in Configuration Manager, use the **Monitoring** workspace in the Configuration Manager console.

> **NOTE**
> The exception to this location is when migrating sites. Monitored this process in the **Migration** node of the **Administration** workspace. For more information, see Operations for migrating to System Center Configuration Manager.

Along with using the Configuration Manager console for monitoring, use the following features:

- Reporting
- Log files.

When you monitor sites, look for signs that indicate problems that require you to take action. For example:

- A backlog of files on site servers and site systems.
- Status messages that indicate an error or a problem.
- Failing intrasite communication.
- Error and warning messages in the system event log on servers.
- Error and warning messages in the Microsoft SQL Server error log.
- Sites or clients that haven't reported status in a long time.
- Sluggish response from the SQL Server database.
- Signs of hardware failure.

If monitoring tasks reveal any signs of problems, investigate the source of the problem. Then quickly repair it to minimize the risk of a site failure.

Monitor common management tasks

Configuration Manager provides built-in monitoring from within the Configuration Manager console.

Alerts

For more information, see Monitor alerts.

Compliance settings

For more information, see How to monitor compliance settings.

Content

For general information about monitoring content, see Manage content and content infrastructure.

For more information about monitoring specific types of content:

- Monitor applications

- Monitor packages and programs
- Monitor content for software updates
- Monitor content for OS deployments

Endpoint Protection

For more information, see How to monitor Endpoint Protection.

OS deployment

For more information, see Monitor OS deployments.

Monitor power management

For more information, see How to monitor and plan for power management.

Monitor software metering

For more information, see Monitor app usage with software metering.

Monitor software updates

For more information, see Monitor software updates.

Monitor the site hierarchy

The **Site Hierarchy** node of the **Monitoring** workspace provides you with an overview of your Configuration Manager hierarchy and intersite links. You can use two views:

- **Hierarchy Diagram**: Displays your hierarchy as a simplified topology map that shows only vital information. For more information, see Hierarchy diagram.
- **Geographical View**: Displays your sites on a geographical map showing site locations that you configure. For more information, see Geographical view.

Use the **Site Hierarchy** node to monitor the health of each site. Also monitor the intersite replication links and their relationship to external factors, such as a geographical location.

Both site status and intersite link status replicate as site data and not global data. When you connect your Configuration Manager console to a child primary site, you can't view the site or link status for other primary sites or their child secondary sites. For example, in a hierarchy with multiple primary sites, when you connect the console to a primary site, you can view the status of child secondary sites, the primary site, and the central administration site. From this view, you can't see the status for other sites below the central administration site.

To control the display in the **Site Hierarchy** node, use the **Configure Settings** action. The hierarchy replicates the settings that you configure in this node.

Hierarchy diagram

The hierarchy diagram displays your sites in a topology map. Select a site, and view a status message summary from that site. Drill through to view status messages, and access the site **Properties**.

To view high-level status for a site or replication link between sites, hover your mouse pointer over the object. Replication link status doesn't replicate globally. To view the replication link details between all primary sites in a hierarchy, connect the console to the central administration site.

The following options modify the hierarchy diagram:

Groups

Configure the number of primary sites and secondary sites that trigger a change in the hierarchy diagram. This change in the display combines the sites into a single object. Then you see the total number of sites and a high-level rollup of status messages and site status. Group configurations don't affect the geographical view.

Favorite sites

Specify individual sites to be a favorite site. A star icon identifies a favorite site in the hierarchy diagram. Favorite sites aren't combined with others sites when you use groups. They're always displayed individually.

Geographical view

The geographical view displays the location of each site on a geographical map. It only displays sites that you configure with a location. When you select a site in this view, it shows replication links to parent or child sites. Unlike the hierarchy diagram view, you can't display site status message or replication link details in this view.

> **NOTE**
>
> To use the geographical view, the computer to which your Configuration Manager console connects must have Internet Explorer installed and be able to access Bing Maps by using the HTTP protocol.

The following option modifies the geographical view:

Site Location

Specify a geographical location for each site using one of the following types:

- A street address
- A place name such as the name of a city
- By latitude and longitude coordinates

For example, to use the latitude and longitude of Redmond, Washington, specify **N 47 40 26.3572 W 122 7 17.4432** as the location of the site. You don't need to specify the symbols for the degree, minutes, or seconds of latitude or longitude. Configuration Manager uses Bing Maps to display the location on the geographical view. Then you can view your hierarchy with the geographical locations. This view provides insight into regional issues that might affect specific sites or intersite replication.

When you specify a location, you can use the **Location** box to search for a specific site in your hierarchy. With the site selected, enter the location as a city name or street address in the **Location** column. Configuration Manager uses Bing Maps to resolve the location.

Next steps

Monitor database replication

Use alerts and the status system for System Center Configuration Manager

5/9/2019 • 15 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configure Alerts, and use the built-in Status System to remain informed about the state of your System Center Configuration Manager deployment.

Status system

All major site components generate status messages that provide feedback on site and hierarchy operations. This information can keep you informed about the health of different site processes. You can tune the alert system to ignore noise for known problems while increasing early visibility for other issues which might need your attention.

By default, the Configuration Manager status system operates without configuration by using settings that are suitable for most environments. However, you can configure the following:

- **Status Summarizers:** You can edit the status summarizers at each site to control the frequency of status messages that generate a status indicator change for the following four summarizers:
  - Application Deployment Summarizer
  - Application Statistics Summarizer
  - Component Status Summarizer
  - Site System Status Summarizer
- **Status Filter Rules:** You can create new status filter rules, modify the priority of rules, disable or enable rules, and delete unused rules at each site.

  > **NOTE**
  > Status filter rules do not support the use of environment variables to run external commands.

- **Status Reporting:** You can configure both server and client component reporting to modify how status messages are reported to the Configuration Manager status system, and specify where status messages are sent.

  > **WARNING**
  > Because the default reporting settings are appropriate for most environments, change them with caution. When you increase the level of status reporting by choosing to report all status details you can increase the amount of status messages to be processed which increases the processing load on the Configuration Manager site. If you decrease the level of status reporting you might limit the usefulness of the status summarizers.

Because the status system maintains separate configurations for each site you must edit each site individually.

Procedures for configuring the status system

To configure status summarizers

1. In the Configuration Manager console navigate to **Administration** > **Site Configuration** >**Sites**, and then

select the site for which you want to configure the status system.

2. On the **Home** tab, in the **Settings** group, click **Status Summarizers**.

3. In the **Status Summarizers** dialog box, select the status summarizer that you want to configure, and then click **Edit** to open the properties for that summarizer. If you are editing the Application Deployment or Application Statistics summarizer, proceed with step 5. If you are editing the Component Status skip to step 6. If you are editing the Site System Status summarizer, skip to step 7.

4. Use the following steps after you open the property page for either the Application Deployment Summarizer or the Application Statistics Summarizer:

   a. On the **General** tab of the summarizers properties page configure the summarization intervals and then click **OK** to close the properties page.

   b. Click **OK** to close the **Status Summarizers** dialog box and complete this procedure.

5. Use the following steps after you open property pages for the Component Status Summarizer:

   a. On the **General** tab of the summarizers' properties page configure the replication and threshold period values.

   b. On the **Thresholds** tab, select the **Message type** you want to configure, and then click the name of a component in the **Thresholds** list.

   c. In the **Status Threshold Properties** dialog box, edit the warning and critical threshold values, and then click **OK**.

   d. Repeat steps 6.b and 6.c as needed and when you are finished, click **OK** to close the summarizer properties.

   e. Click **OK** to close the **Status Summarizers** dialog box and complete this procedure.

6. Use the following steps after you open the property pages for the Site System Status Summarizer:

   a. On the **General** tab of the summarizers' properties page configure the replication and schedule values.

   b. On the **Thresholds** tab, specify values for the **Default thresholds** to configure default thresholds for critical and warning status displays.

   c. To edit the values for specific **Storage objects**, select the object from the **Specific thresholds** list, and then click the **Properties** button to access and edit the storage objects warning and critical thresholds. Click **OK** to close the storage objects properties.

   d. To create a new storage object, click the **Create Object** button and specify the storage objects values. Click **OK** to close the objects properties.

   e. To delete a storage object, select the object and then click the **Delete** button.

   f. Repeat steps 7.b through 7.e as needed. When you are finished, click **OK** to close the summarizer properties.

   g. Click **OK** to close the **Status Summarizers** dialog box and complete this procedure.

To create a status filter rule

1. In the Configuration Manager console navigate to **Administration** > **Site Configuration** >**Sites**, and then select the site where you want to configure the status system.

2. On the **Home** tab, in the **Settings** group, click **Status Filter Rules**. The **Status Filter Rules** dialog box opens.

3. Click **Create**.
4. In the **Create Status Filter Rule Wizard**, on the **General** page, specify a name for the new status filter rule and message-matching criteria for the rule, and then click **Next**.
5. On the **Actions** page, specify the actions to be taken when a status message matches the filter rule, and then click **Next**.
6. On the **Summary** page review the details for the new rule, and then complete the wizard.

> **NOTE**
> Configuration Manager only requires that the new status filter rule has a name. If the rule is created but you do not specify any criteria to process status messages, the status filter rule will have no effect. This behavior allows you to create and organize rules before you configure the status filter criteria for each rule.

To modify or delete a status filter rule

1. In the Configuration Manager console navigate to **Administration** > **Site Configuration** >**Sites**, and then select the site where you want to configure the status system.
2. On the **Home** tab, in the **Settings** group, click **Status Filter Rules**.
3. In the **Status Filter Rules** dialog box, select the rule that you want to modify and then take one of the following actions:
   - Click **Increase Priority** or **Decrease Priority** to change the processing order of the status filter rule. Then select another action or go to step 8 of this procedure to complete this task.
   - Click **Disable** or **Enable** to change the status of the rule. After you change the status of the rule, select another action or go to step 8 of this procedure to complete this task.
   - Click **Delete** if you want do delete the status filter rule from this site, and then click **Yes** to confirm the action. After you delete a rule, select another action or go to step 8 of this procedure to complete this task.
   - Click **Edit** if you want to change the criteria for the status message rule, and continue to step 5 of this procedure.
4. On the **General** tab of the status filter rule properties dialog box, modify the rule and message-matching criteria.
5. On the **Actions** tab, modify the actions to be taken when a status message matches the filter rule.
6. Click **OK** to save the changes.
7. Click **OK** to close the **Status Filter Rules** dialog box.

To configure status reporting

1. In the Configuration Manager console navigate to **Administration** > **Site Configuration** > **Sites**, and then select the site where you want to configure the status system.
2. On the **Home** tab, in the **Settings** group, click **Configure Site Components**, and select **Status Reporting**.
3. In the **Status Reporting Component Properties** dialog box, specify the server and client component status messages that you want to report or log:
   a. Configure **Report** to send status messages to the Configuration Manager status message system.
   b. Configure **Log** to write the type and severity of status messages to the Windows event log.
4. Click **OK**.

Monitor the status system of Configuration Manager

System status in Configuration Manager provides an overview of the general operations of sites and site server operations of your hierarchy. It can reveal operational problems for site system servers or components, and you can use the system status to review specific details for different Configuration Manager operations. You monitor system status from the **System Status** node of the **Monitoring** workspace in the Configuration Manager console.

Most Configuration Manager site system roles and components generate status messages. Status messages details are logged in each components operational log, but are also submitted to the site database where they are summarized and presented in a general rollup of each component or site systems health. These status message rollups provide information details for regular operations and warnings and error details. You can configure the thresholds at which warnings or errors are triggered and fine-tune the system to ensure rollup information ignores known issues that are not relevant to you while calling attention to actual problems on servers or for component operations that you might want to investigate.

System status is replicated to other sites in a hierarchy as site data, not global data. This means you can only see the status for the site to which your Configuration Manager console connects, and any child sites below that site. Therefore, consider connecting your Configuration Manager console to the top-level site of your hierarchy when you view system status.

Use the following table to identify the different system status views and when to use each one.

NODE	MORE INFORMATION
Site Status	Use this node to view a rollup of the status of each site system to review the health of each site system server. Site system health is determined by thresholds that you configure for each site in the **Site System Status Summarizer**. You can view status messages for each site system, set thresholds for status messages, and manage the operation of the components on site systems by using the **Configuration Manager Service Manager**.
Component Status	Use this node to view a rollup of the status of each Configuration Manager component to review the component's operational health. Component health is determined by thresholds that you configure for each site in the **Component Status Summarizer**. You can view status messages for each component, set thresholds for status messages, and manage the operation of components by using the **Configuration Manager Service Manager**.
Conflicting Records	Use this node to view status messages about clients that might have conflicting records. Configuration Manager uses the hardware ID to attempt to identify clients that might be duplicates and alert you to the conflicting records. For example, if you have to reinstall a computer, the hardware ID would be the same, but the GUID that Configuration Manager uses might be changed.

NODE	MORE INFORMATION
Status Message Queries	Use this node to query status messages for specific events and related details. You can use status message queries to find the status messages related to specific events. You can often use status message queries to identify when a specific component, operation, or Configuration Manager object was modified, and the account that was used to make the modification. For example, you can run the built-in query for **Collections Created, Modified, or Deleted** to identify when a specific collection was created, and the user account used to create the collection.

Manage site status and component status

Use the following information to manage the site status and component status:

- To configure thresholds for the status system, see Procedures for configuring the status system.
- To manage individual components in Configuration Manager, use the **Configuration Manager Service Manager**.

View status messages

You can view the status messages for individual site system servers and components.

To view status messages in the Configuration Manager console, select a specific site system server or component, and then click **Show Messages**. When you view messages, you can select to view specific message types or messages from a specified period of time, and you can filter the results based on the status messages details.

Alerts

Configuration Manager alerts are generated by some operations when a specific condition occurs.

- Typically, alerts are generated when an error occurs that you must resolve
- Alerts might be generated to warn you that a condition exists so that you can continue to monitor the situation
- Some alerts you configure, such as alerts for Endpoint Protection and client status, while other alerts are configured automatically
- You can configure subscriptions to alerts which can then send details by email, increasing awareness of key issues

  Use the following table to find information about how to configure alerts and alert subscriptions in Configuration Manager:

ACTION	MORE INFORMATION
Configure Endpoint Protection alerts for a collection	See **How to Configure Alerts for Endpoint Protection in Configuration Manager** in Configuring Endpoint Protection in System Center Configuration Manager
Configure client status alerts for a collection	See How to configure client status in System Center Configuration Manager.
Manage Configuration Manager alerts	See the section Management tasks for alerts in this topic.

ACTION	MORE INFORMATION
Configure email subscriptions to alerts	See the section Management tasks for alerts in this topic..
Monitor alerts	See the section Monitor alerts

Management tasks for alerts

To manage general alerts

1. In the Configuration Manager console navigate to **Monitoring** > **Alerts**, and then select a management task.

   Use the following table for more information about the management tasks that might require some information before you select them.

MANAGEMENT TASK	DETAILS
Configure	Opens the <*alert name*>**Properties** dialog box where you can modify the name, severity, and thresholds for the selected alert. If you change the severity of the alert, this configuration affects how the alerts are displayed in the Configuration Manager console.
Edit Comment	Enter a comment for the selected alerts. These comments display with the alert in the Configuration Manager console.
Postpone	Suspends the monitoring of the alert until the specified date is reached. At that time, the state of the alert is updated. You can only postpone an alert when it is enabled.
Create subscription	Opens the **New Subscription** dialog box where you can create an email subscription to the selected alert.

To configure client status alerts for a collection

1. In the Configuration Manager console, click **Assets and Compliance** > **Device Collections**.
2. In the **Device Collections** list, select the collection for which you want to configure alerts and then, in the **Home** tab, in the **Properties** group, click **Properties**.

   > **NOTE**
   > You cannot configure alerts for user collections.

3. On the **Alerts** tab of the <*Collection Name*>**Properties** dialog box, click **Add**.

   > **NOTE**
   > The **Alerts** tab is only visible if the security role you are associated with has permissions for alerts.

4. In the **Add New Collection Alerts** dialog box, choose the alerts that you want generated when client status thresholds fall below a specific value, then click **OK**.
5. In the **Conditions** list of the **Alerts** tab, select each client status alert and then specify the following information.

   - **Alert Name** - Accept the default name or enter a new name for the alert.

- **Alert Severity** - From the drop-down list, choose the alert level that will be displayed in the Configuration Manager console.
- **Raise alert** - Specify the threshold percentage for the alert.

6. Click **OK** to close the <*Collection Name*>**Properties** dialog box.

To configure email notification for alerts

1. In the Configuration Manager console navigate to **Monitoring** > **Alerts** > **Subscriptions**.
2. On the **Home** tab, in the **Create** group, click **Configure Email Notification**.
3. In the **Email Notification Component Properties** dialog box, specify the following information:
   - **Enable email notification for alerts**: Select this check box to enable Configuration Manager to use an SMTP server to send email alerts.
   - **FQDN or IP Address of the SMTP server to send email alerts**: Enter the fully qualified domain name (FQDN) or IP address and the SMTP port for the email server that you want to use for these alerts.
   - **SMTP Server Connection Account**: Specify the authentication method for Configuration Manager to use to connect the email server.
   - **Sender address for email alerts**: Specify the email address from which alert emails are sent.
   - **Test SMTP Server**: Sends a test email to the email address specified in **Sender address for email alerts**.
4. Click **OK** to save the settings and to close the **Email Settings Component Properties** dialog box.

To subscribe to email alerts

1. In the Configuration Manager console navigate to **Monitoring** > **Alerts**.
2. Select an alert and then, on the **Home** tab, in the **Subscription** group, click **Create subscription**.
3. In the **New Subscription** dialog box, specify the following information:
   - **Name**: Enter a name to identify the email subscription. You can use up to 255 characters.
   - **Email address**: Enter the email addresses that you want the alert sent to. You can separate multiple email addresses with a semicolon.
   - **Email language**: In the list, specify the language for the email.
4. Click **OK** to close the **New Subscription** dialog box and to create the email subscription.

> **NOTE**
> You can delete and edit subscriptions in the **Monitoring** workspace when you expand the **Alerts** node, and then click the **Subscriptions** node.

Monitor alerts

You can view alerts in the **Alerts** node of the **Monitoring** workspace. Alerts have one of the following alert states:

- **Never triggered**: The condition of the alert has not been met.
- **Active**: The condition of the alert is met.
- **Canceled**: The condition of an active alert is no longer met. This state indicates that the condition that caused the alert is now resolved.

- **Postponed**: An administrative user has configured Configuration Manager to evaluate the state of the alert at a later time.
- **Disabled**: The alert has been disabled by an administrative user. When an alert is in this state, Configuration Manager does not update the alert even if the state of the alert changes.

  You can take one of the following actions when Configuration Manager generates an alert:

- Resolve the condition that caused the alert, for example, you resolve a network issue or a configuration issue that generated the alert. After Configuration Manager detects that the issue no longer exists, the alert state changes to **Cancel**.
- If the alert is a known issue, you can postpone the alert for a specific length of time. At that time, Configuration Manager updates the alert to its current state.

  You can postpone an alert only when it is active.

- You can edit the **Comment** of an alert so that other administrative users can see that you are aware of the alert. For example, in the comment you can identify how to resolve the condition, provide information about the current status of the condition, or explain why you postponed the alert.

Health attestation for System Center Configuration Manager

5/9/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Administrators can view the status of Windows 10 Device Health Attestation in the Configuration Manager console. Device health attestation lets the administrator ensure that client computers have the following trustworthy BIOS, TPM, and boot software configurations enabled:

- Early-launch antimalware - Early launch anti-malware (ELAM) protects your computer when it starts up and before third-party drivers initialize. How to turn on ELAM
- BitLocker - Windows BitLocker Drive Encryption is software that lets you encrypt all data stored on the Windows operating system volume. How to turn on BitLocker
- Secure Boot - Secure Boot is a security standard developed by members of the PC industry to help make sure that your PC boots using only software that is trusted by the PC manufacturer. Learn more about Secure Boot
- Code Integrity - Code Integrity is a feature that improves the security of the operating system by validating the integrity of a driver or system file each time it is loaded into memory. Learn about Code Integrity

This functionality is available for PCs and on-premises resources managed by Configuration Manager and mobile devices managed with Microsoft Intune. Administrators can specify whether reporting is done via the cloud or on-premises infrastructure. On-premises device health attestation monitoring enables administrator to monitor client PCs without internet access.

Enable Health Attestation

Requirements:

- Client devices running Windows 10 version 1607 or Windows Server 2016 version 1607 with Device Health Attestation enabled.
- TPM 1.2 or TPM 2 enabled devices.
- When using cloud management, communication between the Configuration Manager client agent and the management point with *has.spserv.microsoft.com* (port 443) Health Attestation service (cloud management). When on-premises, the client must be able to communicate with the device health attestation-enabled management point.

How to enable Health Attestation service communication on Configuration Manager client computers

Use this procedure to enable device health attestation monitoring for devices that connect to the internet.

1. In the Configuration Manager console, choose **Administration** > **Overview** > **Client Settings**. Select the tab for **Computer Agent** settings.
2. In the **Default Settings** dialog box, select **Computer Agent** and then scroll down to **Enable communication with Health Attestation Service**
3. Set **Enable communication with Health Attestation Service** to **Yes**, and then click **OK**.
4. Target the collections of devices that should report device health.

How to enable on-premises Health Attestation service communication on Configuration Manager client computers

Use this procedure to enable device health attestation monitoring for on-premises devices that don't connect to the internet.

Starting with Configuration Manager 1702, the on-premises device health attestation service URL can be configured on the management point to support client devices without internet access.

1. In the Configuration Manager console, navigate **Administration** > **Overview** > **Site Configuration** > **Sites**.
2. Right-click the primary or secondary site with the management point that support on-premises device health attestation clients, and select **Configure site components** > **Management Point**. The **Management Point Component Properties** page opens.
3. On the **Advanced Options** tab, select **Add** and specify a valid on-premises device health attestation service URL. You can add multiple URLs. If multiple on-premises URLs are specified, clients receive the full set and randomly choose which to use.
4. In the Configuration Manager console, choose **Administration** > **Overview** > **Client Settings**. Select the tab for **Computer Agent** settings.
5. Scroll down to **Enable communication with Health Attestation Service**, and set to **Yes**.
6. Click the **Use on-premises Health Attestaion Service** option, and set to **Yes**.
7. Target the collections of devices that should report device health with the client agent settings to enable device health attestation reporting.

You can also **Edit** or **Remove** device health attestation service URLs.

> **NOTE**
> If you used device health attestation prior to upgrading to Configuration Manager 1702, the on-premises URLs specified in the client agent settings is pre-populate in the management point properties during the upgrade. On-premises clients will continue to use the URL specified in client agent settings until they are upgraded. They will then switch to one of the URLs specified on the management point.

Monitor device health attestation

1. To view the device health attestation view, in the Configuration Manager console go to the **Monitoring** workspace of, click **Security** node, and then click **Health Attestation**.
2. Device Health Attestation is displayed.

Configuration Manager Device Health Attestation displays the following:

- **Health Attestation Status** - Shows the share of devices in compliant, noncompliant, error, and unknown states
- **Devices Reporting Health Attestation** - Shows the percentage of devices reporting Health Attestation status
- **Noncompliant Devices by Client Type** - Shows share of mobile devices and computers that are noncompliant
- **Top Missing Health Attestation Settings** - Shows the number of devices missing the health attestation setting, listed per setting

Client Device Health Attestation status can be used to define rules for conditional access in compliance policies for devices managed by Configuration Manager with Microsoft Intune. For details, see Manage device compliance policies in System Center Configuration Manager.

Monitor database replication

8/12/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Monitor details for database replication with the **Database Replication** node in the **Monitoring** workspace of the Configuration Manager console. You can monitor the status of replication links between sites. It also shows initialization and replication of replication groups for the site to which you connect.

> **TIP**
> Although a **Database Replication** node also appears under the **Hierarchy Configuration** node in the **Administration** workspace, you can't view the replication status for database replication links from that location.

Replication link status

Database replication between sites involves the replication of several sets of information, called *replication groups*. Each replication group sends and receives data with different priorities. By default, you can't modify the data contained in a replication group and the frequency of replication.

When a replication link is active, and its status isn't failed or degraded, all groups replicate quickly. If one or more groups fail to complete replication in the expected period of time, the link displays as *degraded*. Degraded links can still function, but you should monitor them to make sure they return to active status. Investigate them to make sure additional degradation or replication failures don't occur.

For each replication link, specify the number of times that an unsuccessfully replicated group retries. After this number of retries, the site sets the status of the link to degraded or failed. Even if all but one group replicates successfully, the site sets the status of the link to degraded or failed. It sets this status because the one replication group fails to complete replication in the specified number of attempts. For more information, see the Database replication thresholds.

Use the following information to understand the status of replication links that might require further investigation:

Link is active

No problems have been detected, and communication across the link is current.

While a parent site is updating to a new version, and you view the link status from the child site, the link status displays as active. After the update, until the child site is at the same version as the parent site, the link status displays as active when viewed from the parent site. When viewed from the child site, it displays as being configured.

Link is degraded

Replication is functional, but at least one replication object or group is delayed. Monitor links that are in this state. Review information from both sites on the link for indications that the link might fail.

A link can also display a status of degraded when the site that receives replicated data is unable to quickly commit the data to the database. This behavior happens when large volumes of data replicate. For example, you deploy a software update to a large number of computers. The parent site on the link might take some time to process this volume of replicated data. A processing lag at the parent site results in it setting the link status to degraded until it can successfully process the backlog of data.

Link has failed

Replication isn't functional. It's possible that a replication link might recover without further action. To investigate and help remediate replication on this link, use the Replication Link Analyzer (RLA).

This status can also indicate a problem with the physical network between the parent and child site on the replication link.

Monitor replication status

Use the **Database Replication** node in the **Monitoring** workspace to view the status for a replication link. View details about the database at each site on the replication link. You can also view details about replication groups. To view these details, select a replication link, and then select the appropriate tab for the replication status you want to view.

The following sections give details about the different tabs for replication status:

Summary

View high-level information about the replication of site data and global data between the two sites on a link.

Select **View reports for historical traffic data** to view a report that shows details about the network bandwidth used by replication across the link.

Parent Site

For the parent site on a replication link, view details about the database, which include:

- Firewall ports for the SQL Server
- Free disk space
- Database file locations
- Certificates

Child Site

For the child site on a replication link, view details about the database, which include:

- Firewall ports for the SQL Server
- Free disk space
- Database file locations
- Certificates

Initialization Detail

View the initialization status for groups that replicate across the link. This information can help you identify when initialization of replication data is in progress or has failed.

Use this information to identify when a site might be in *interoperability mode*. Interoperability mode is when the child site doesn't run the same version of Configuration Manager as the parent site.

Replication Detail

View the replication status for each group that replicates across the link. Use this information to help identify problems or delays for the replication of specific data. It can help determine the appropriate database replication thresholds for this link. For more information, see Database replication thresholds.

> **TIP**
> Replication groups for site data are sent only from the child site to the parent site. Replication groups for global data replicate in both directions.

Replication Link Analyzer

Configuration Manager includes the **Replication Link Analyzer** (RLA), which you use to analyze and repair replication issues. Use RLA to remediate link failures when replication fails. It's also useful when replication stops working but the site hasn't yet reported it as failed.

Use RLA to remediate replication issues between the following computers in the hierarchy:

- Between a site server and the site database server
- Between a site's database server and another site's database server, otherwise known as intersite replication

> **NOTE**
> The direction of the replication failure doesn't matter.

Run RLA in either the Configuration Manager console or at a command prompt:

- To run in the Configuration Manager console: Go to the **Monitoring** workspace, and select the **Database Replication** node. Select the replication link that you want to analyze, and then in ribbon, select **Replication Link Analyzer**.
- To run at a command prompt, type the following command:

```
%ProgramFiles(x86)%\Microsoft Configuration
Manager\AdminConsole\bin\Microsoft.ConfigurationManager.ReplicationLinkAnalyzer.Wizard.exe <source site
server FQDN> <destination site server FQDN>
```

When you run RLA, it detects problems by using a series of diagnostic rules and checks. You view the problems that the tool identifies. When it has instructions to resolve an issue, it displays them. If RLA can automatically remediate a problem, it presents you with that option.

When RLA finishes, it saves the results in the following XML-based report and a log file on the desktop of the user who runs the tool:

- ReplicationAnalysis.xml
- ReplicationLinkAnalysis.log

RLA stops the following services while it remediates some problems. It restarts these services when remediation is complete:

- SMS_SITE_COMPONENT_MANAGER
- SMS_EXECUTIVE

If RLA fails to complete remediation, restart these services on the site server if necessary.

RLA logs all investigation and remediation actions to provide additional details that it doesn't display in the wizard.

RLA prerequisites

The account that you use to run RLA must have the following permissions:

- Local administrator rights on each computer that's involved in the replication link.

- Sysadmin rights on each SQL Server database that's involved in the replication link.

> **NOTE**
>
> The account doesn't require a specific Configuration Manager role-based administration security role. An administrative user with access to the **Database Replication** node can run the tool in the Configuration Manager console. A system administrator with sufficient rights to each computer can run the tool at a command prompt.

RLA known issue

RLA generates SQL Server Service Broker (SSB) certificate errors for primary sites that upgraded from System Center 2012 Configuration Manager. This issue is because of changes in the names of the certificates in Configuration Manager current branch. You can safely ignore these errors.

Monitoring database replication

Monitor high-level site-to-site database replication status

1. In the Configuration Manager console, go to the **Monitoring** workspace.
2. Select the **Site Hierarchy** node to open the **Hierarchy Diagram** view.
3. Hover the mouse pointer on the line between the two sites. View the status of global and site data replication for these sites.

Monitor the status of a replication link

1. In the Configuration Manager console, go to the **Monitoring** workspace.
2. Select the **Database Replication** node, and then select the replication link that you want to monitor. Then select the appropriate tab to view different details about the replication status for that link.

Troubleshoot SQL replication

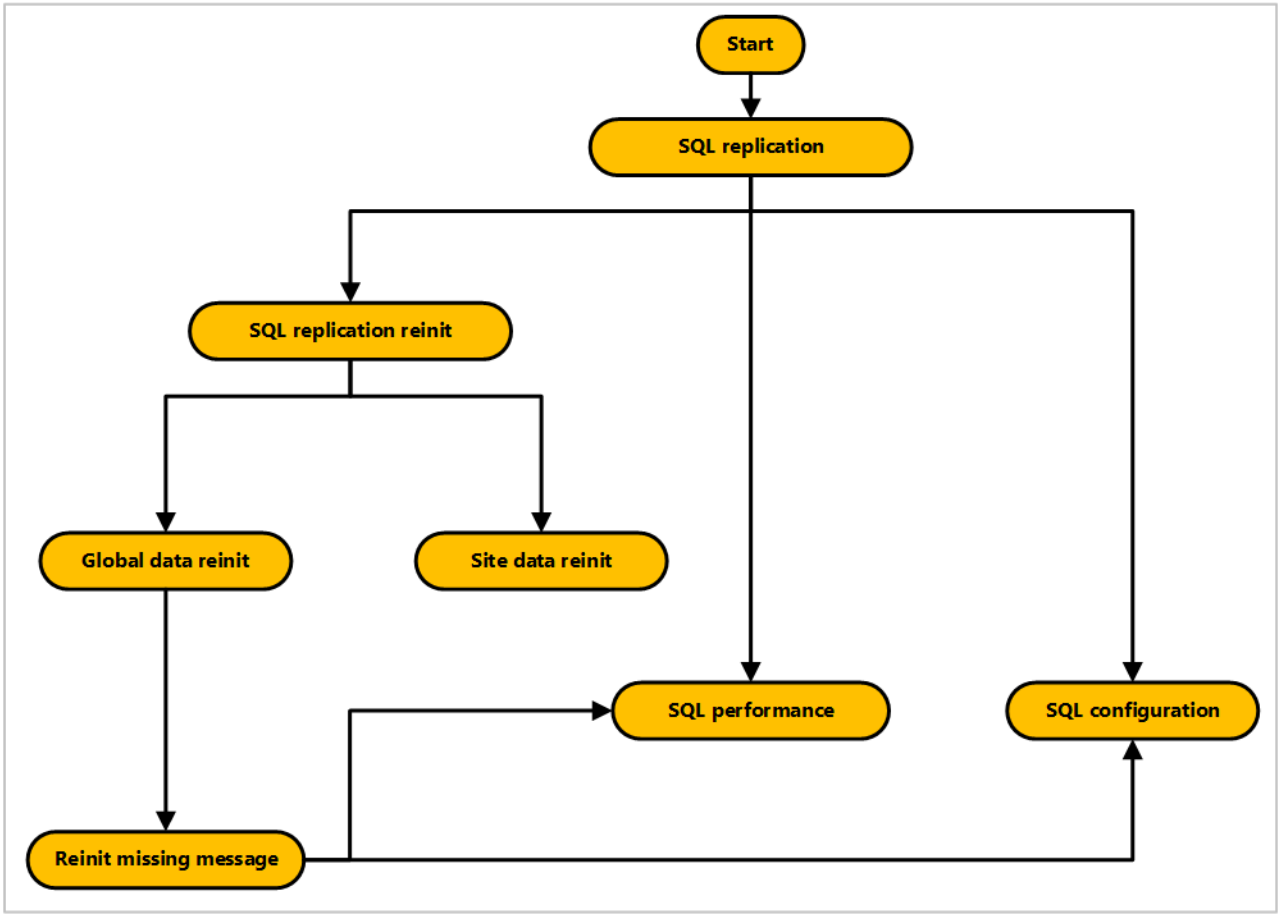
8/12/2019 • 2 minutes to read • Edit Online

In a multi-site hierarchy, Configuration Manager uses SQL replication to transfer data between sites. For more information, see Database replication.

To better understand and help troubleshoot issues with SQL replication, use these diagrams.

- SQL replication
- SQL configuration
- SQL performance
- SQL replication reinitialization (reinit)
- Global data reinit
- Site data reinit
- Reinit missing message

These troubleshooting diagrams are interconnected. Use the following diagram to understand their relationships:



For more information, see the following series of blogs from Microsoft Support:

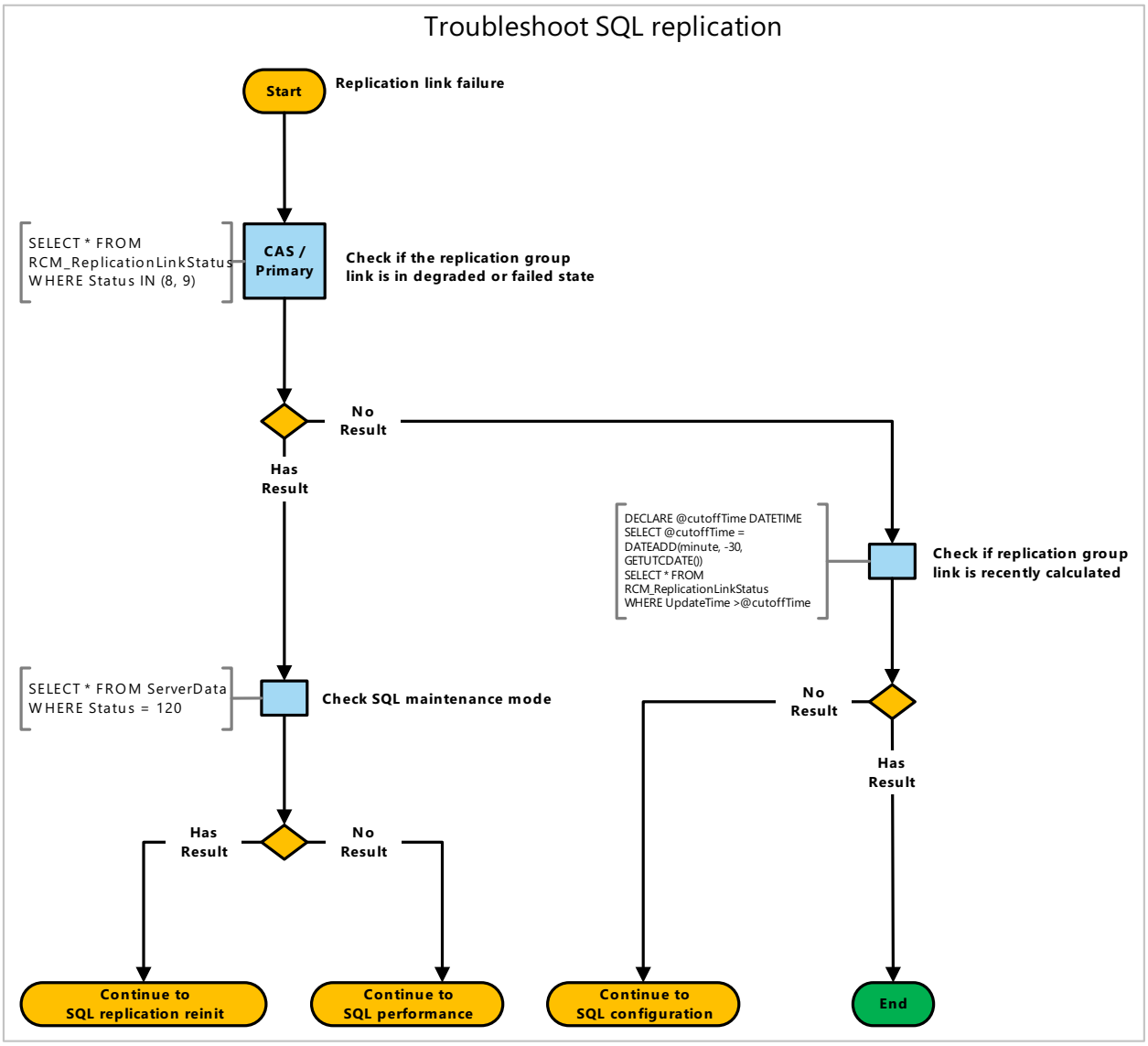
- ConfigMgr DRS Synchronization Internals
- ConfigMgr 2012 Data Replication Service (DRS) Unleashed
- ConfigMgr 2012 DRS – Troubleshooting FAQs
- ConfigMgr 2012 DRS Initialization Internals
- ConfigMgr 2012: DRS and SQL service broker certificate issues

SQL replication

8/12/2019 • 2 minutes to read • Edit Online

In a multi-site hierarchy, Configuration Manager uses SQL replication to transfer data between sites. For more information, see Database replication.

Use the following diagram to start troubleshooting SQL replication when a link fails:



Queries

This diagram uses the following queries:

Check if the replication group link is in degraded or failed state

```
SELECT * FROM RCM_ReplicationLinkStatus
WHERE Status IN (8, 9)
```

Check if replication group link is recently calculated

```
DECLARE @cutoffTime DATETIME
SELECT @cutoffTime = DATEADD(minute, -30, GETUTCDATE())
SELECT * FROM RCM_ReplicationLinkStatus
WHERE UpdateTime >@cutoffTime
```

Check SQL maintenance mode

```
SELECT * FROM ServerData
WHERE Status = 120
```

Next steps

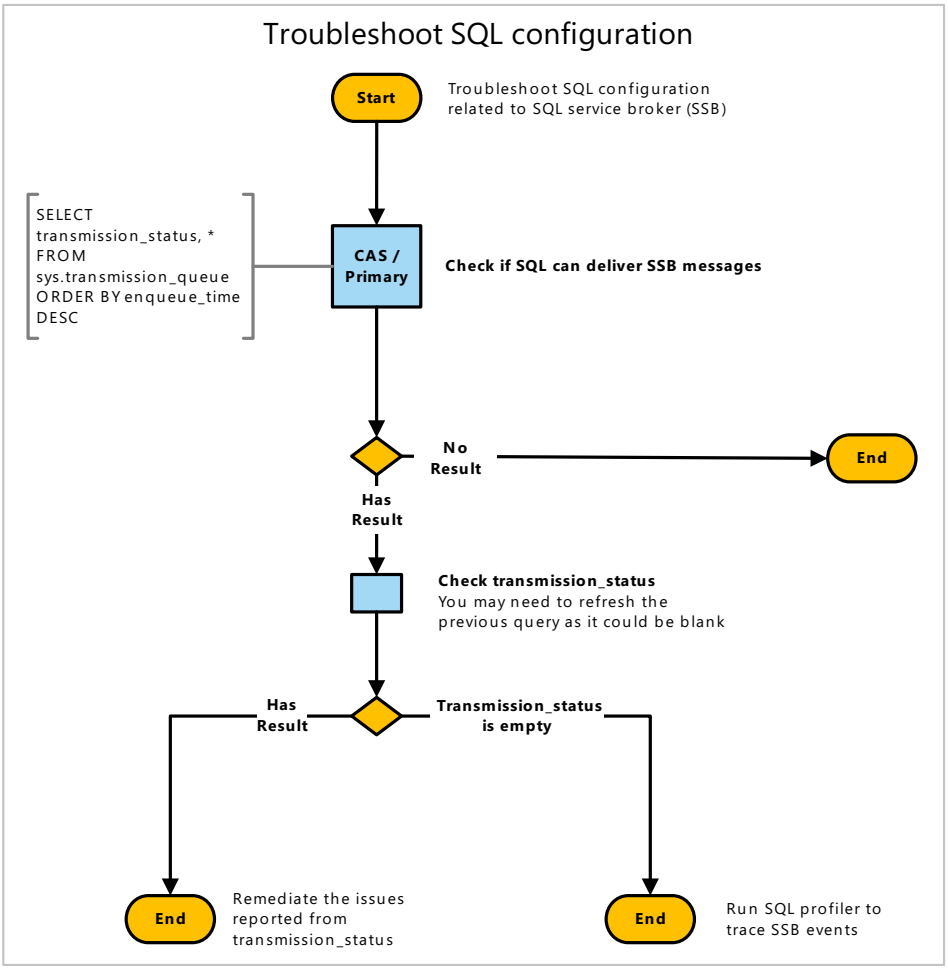
- SQL replication reinitialization (reinit)
- SQL performance
- SQL configuration

SQL configuration

8/12/2019 • 2 minutes to read • Edit Online

In a multi-site hierarchy, Configuration Manager uses SQL replication to transfer data between sites. For more information, see Database replication.

Use the following diagram to start troubleshooting SQL configuration related to SQL Service Broker:



Queries

This diagram has the following queries and actions:

Check if SQL can deliver SSB messages

```
SELECT transmission_status, *
FROM sys.transmission_queue
ORDER BY enqueue_time DESC
```

Remediation actions

Remediate the issues reported from transmission_status

Common issues:

- Firewall configuration
- Network configuration

- SSB certificate misconfigured

Run SQL profiler to trace SSB events

Run SQL profiler on the CAS and primary site database to trace events related to the SQL Service Broker:

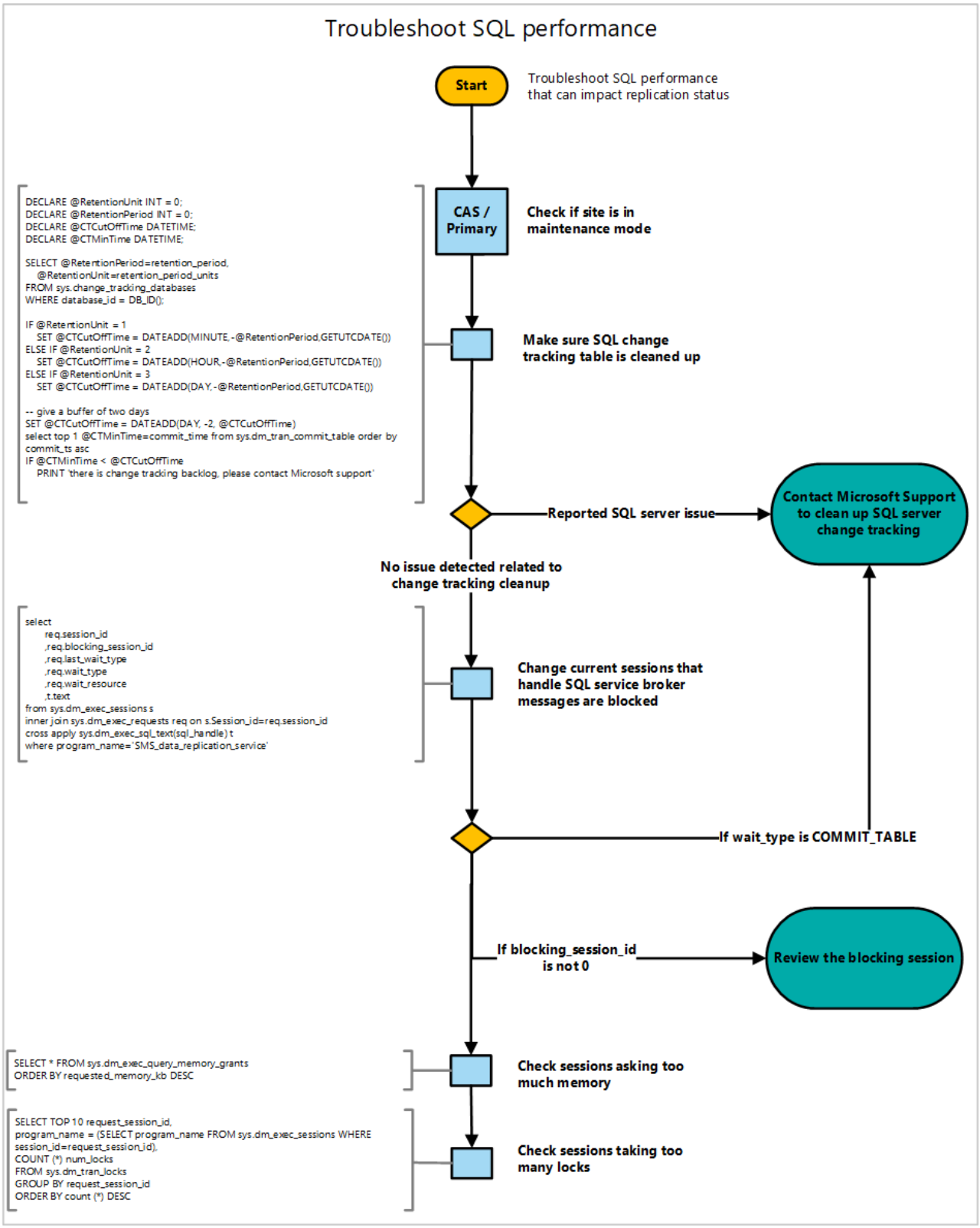
- **Audit Broker Login**
- **Audit Broker Conversation**
- Events in **Broker** category

SQL performance

8/12/2019 • 2 minutes to read • Edit Online

In a multi-site hierarchy, Configuration Manager uses SQL replication to transfer data between sites. For more information, see Database replication.

Use the following diagram to start troubleshooting SQL performance that can impact replication status:



Queries

This diagram uses the following queries:

Make sure SQL change tracking table is cleaned up

```
DECLARE @RetentionUnit INT = 0;
DECLARE @RetentionPeriod INT = 0;
DECLARE @CTCutOffTime DATETIME;
DECLARE @CTMinTime DATETIME;

SELECT @RetentionPeriod=retention_period,
    @RetentionUnit=retention_period_units
FROM sys.change_tracking_databases
WHERE database_id = DB_ID();

IF @RetentionUnit = 1
    SET @CTCutOffTime = DATEADD(MINUTE,-@RetentionPeriod,GETUTCDATE())
ELSE IF @RetentionUnit = 2
    SET @CTCutOffTime = DATEADD(HOUR,-@RetentionPeriod,GETUTCDATE())
ELSE IF @RetentionUnit = 3
    SET @CTCutOffTime = DATEADD(DAY,-@RetentionPeriod,GETUTCDATE())

-- give a buffer of two days
SET @CTCutOffTime = DATEADD(DAY, -2, @CTCutOffTime)
select top 1 @CTMinTime=commit_time from sys.dm_tran_commit_table order by commit_ts asc
IF @CTMinTime < @CTCutOffTime
    PRINT 'there is change tracking backlog, please contact Microsoft support'
```

Change current sessions that handle SQL service broker messages are blocked

```
select
       req.session_id
       ,req.blocking_session_id
       ,req.last_wait_type
       ,req.wait_type
       ,req.wait_resource
       ,t.text
from sys.dm_exec_sessions s
inner join sys.dm_exec_requests req on s.Session_id=req.session_id
cross apply sys.dm_exec_sql_text(sql_handle) t
where program_name='SMS_data_replication_service'
```

Check sessions asking too much memory

```
SELECT * FROM sys.dm_exec_query_memory_grants
ORDER BY requested_memory_kb DESC
```

Check sessions taking too many locks

```
SELECT TOP 10 request_session_id,
program_name = (SELECT program_name FROM sys.dm_exec_sessions WHERE session_id=request_session_id),
COUNT (*) num_locks
FROM sys.dm_tran_locks
GROUP BY request_session_id
ORDER BY count (*) DESC
```

See also

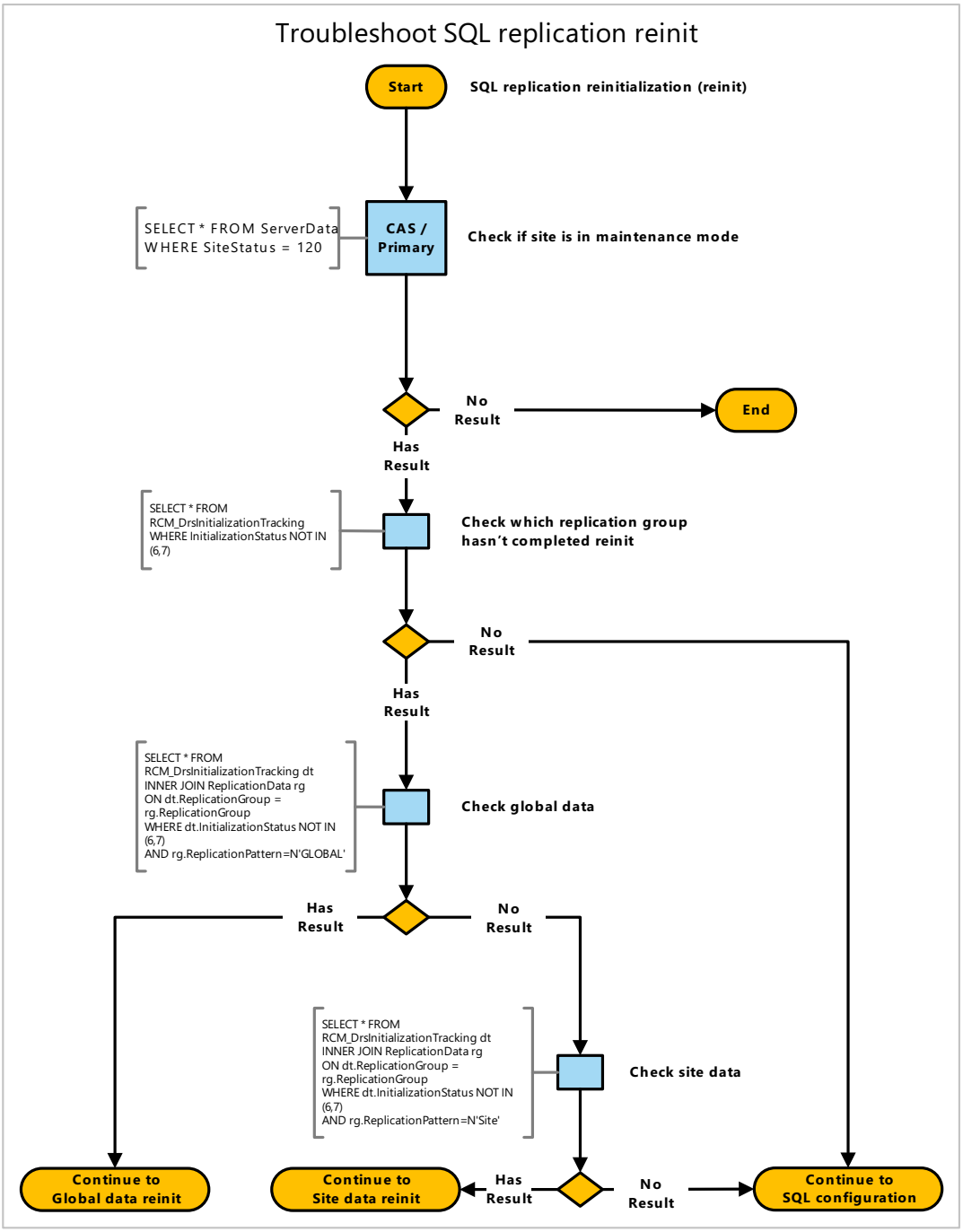
SQL configuration

SQL replication reinit

8/12/2019 • 2 minutes to read • Edit Online

In a multi-site hierarchy, Configuration Manager uses SQL replication to transfer data between sites. For more information, see Database replication.

Use the following diagram to start troubleshooting SQL replication reinitialization (reinit):



Queries

This diagram uses the following queries:

Check if site is in maintenance mode

```
SELECT * FROM ServerData
WHERE Status = 120
```

Check which replication group hasn't completed reinit

```
SELECT * FROM RCM_DrsInitializationTracking
WHERE InitializationStatus NOT IN (6,7)
```

Check global data

```
SELECT * FROM RCM_DrsInitializationTracking dt
INNER JOIN ReplicationData rg
ON dt.ReplicationGroup = rg.ReplicationGroup
WHERE dt.InitializationStatus NOT IN (6,7)
AND rg.ReplicationPattern=N'GLOBAL'
```

Check site data

```
SELECT * FROM RCM_DrsInitializationTracking dt
INNER JOIN ReplicationData rg
ON dt.ReplicationGroup = rg.ReplicationGroup
WHERE dt.InitializationStatus NOT IN (6,7)
AND rg.ReplicationPattern=N'Site'
```

Next steps

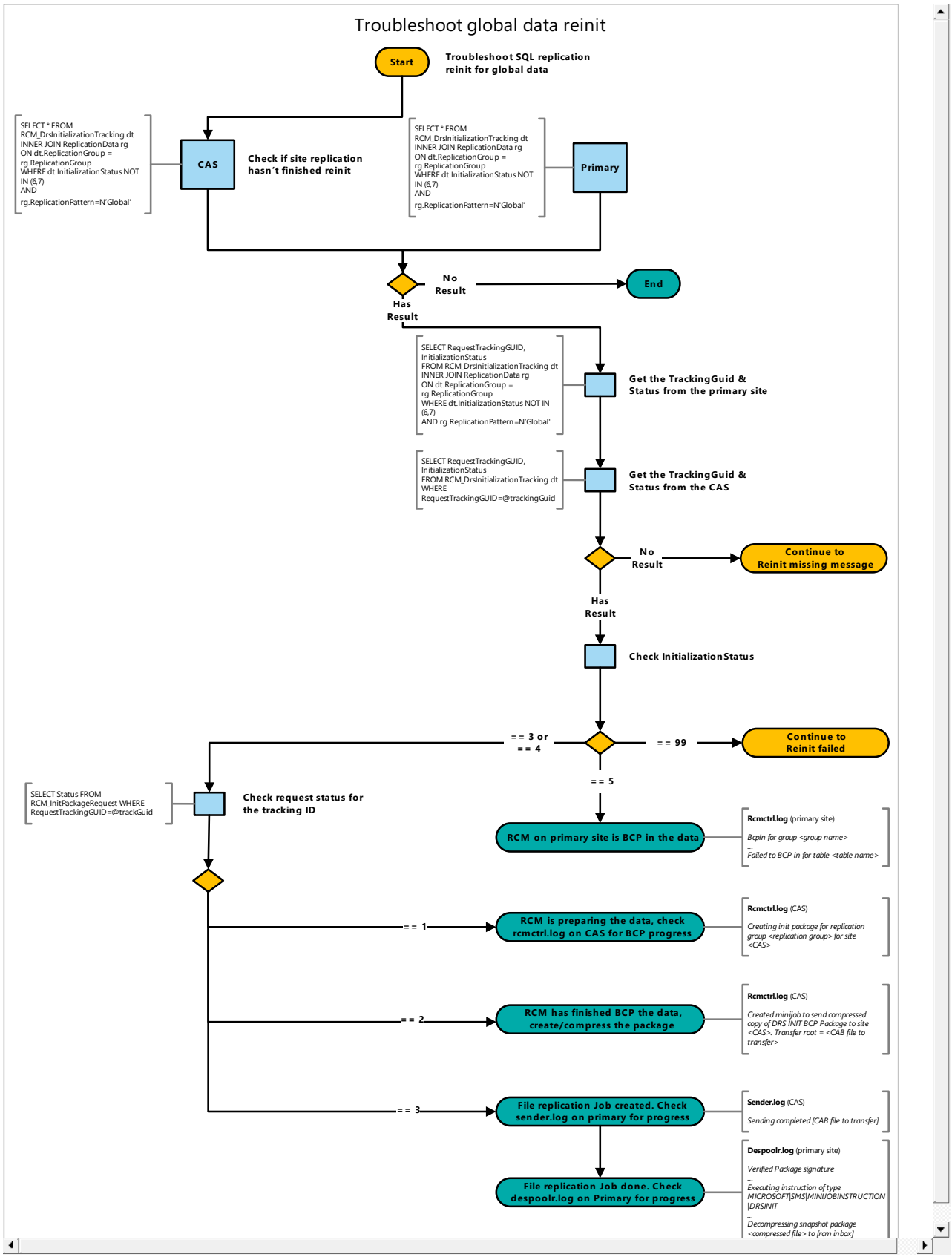
- Global data reinit
- Site data reinit
- SQL configuration

Troubleshoot global data reinit

9/11/2019 • 2 minutes to read • Edit Online

In a multi-site hierarchy, Configuration Manager uses SQL replication to transfer data between sites. For more information, see Database replication.

Use the following diagram to start troubleshooting SQL replication reinitialization (reinit) for global data in a Configuration Manager hierarchy:



Queries

This diagram uses the following queries:

Check if site replication hasn't finished reinit

```
SELECT * FROM RCM_DrsInitializationTracking dt
INNER JOIN ReplicationData rg
ON dt.ReplicationGroup = rg.ReplicationGroup
WHERE dt.InitializationStatus NOT IN (6,7)
AND rg.ReplicationPattern=N`Global'
```

Get the TrackingGuid & Status from the primary site

```
SELECT RequestTrackingGUID, InitializationStatus
FROM RCM_DrsInitializationTracking dt
INNER JOIN ReplicationData rg
ON dt.ReplicationGroup = rg.ReplicationGroup
WHERE dt.InitializationStatus NOT IN (6,7)
AND rg.ReplicationPattern=N`Global'
```

Get the TrackingGuid & Status from the CAS

```
SELECT RequestTrackingGUID, InitializationStatus
FROM RCM_DrsInitializationTracking dt
WHERE RequestTrackingGUID=@trackingGuid
```

Check request status for the tracking ID

```
SELECT Status FROM RCM_InitPackageRequest
WHERE RequestTrackingGUID=@trackGuid
```

Next steps

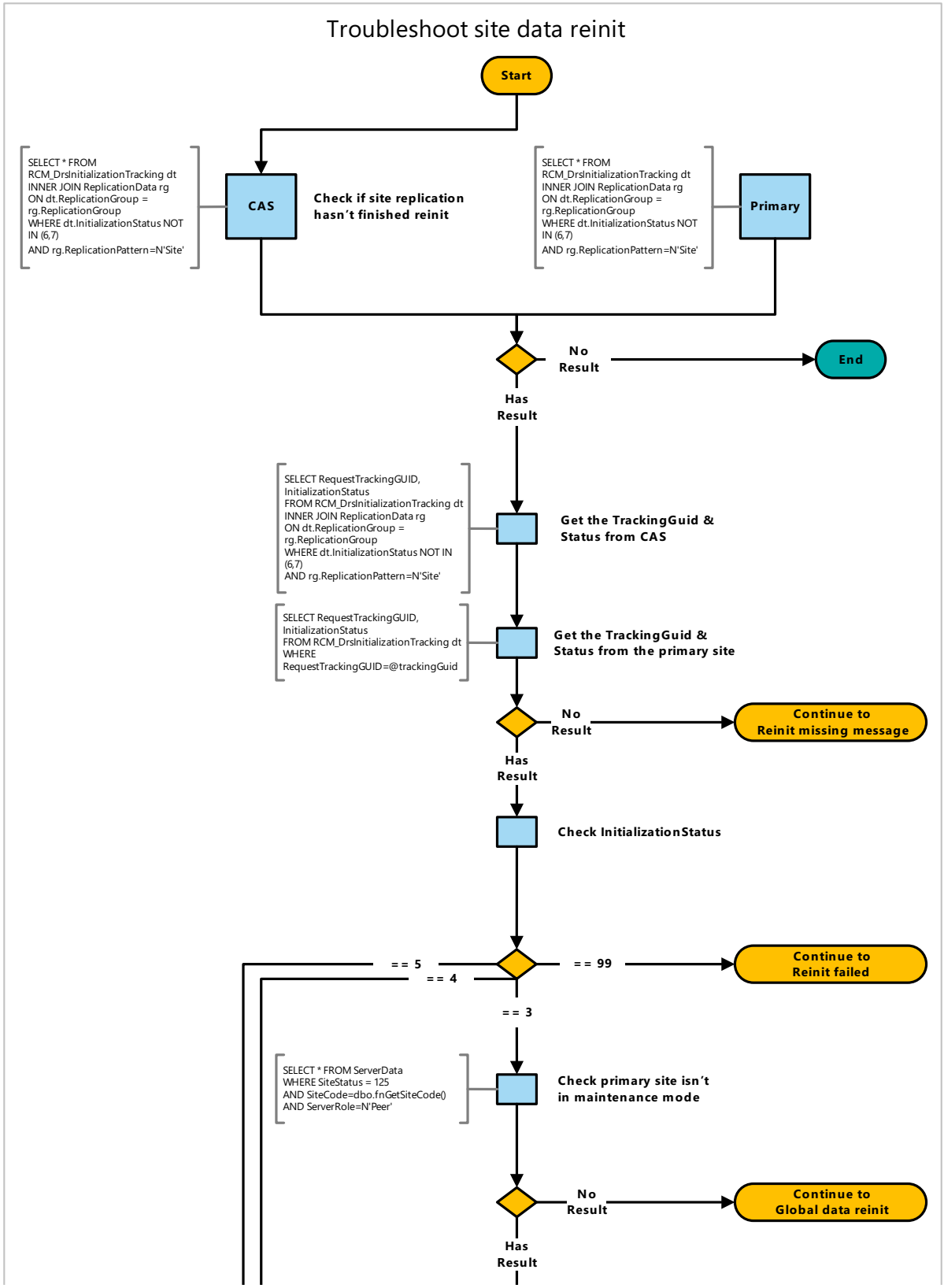
- Reinit missing message

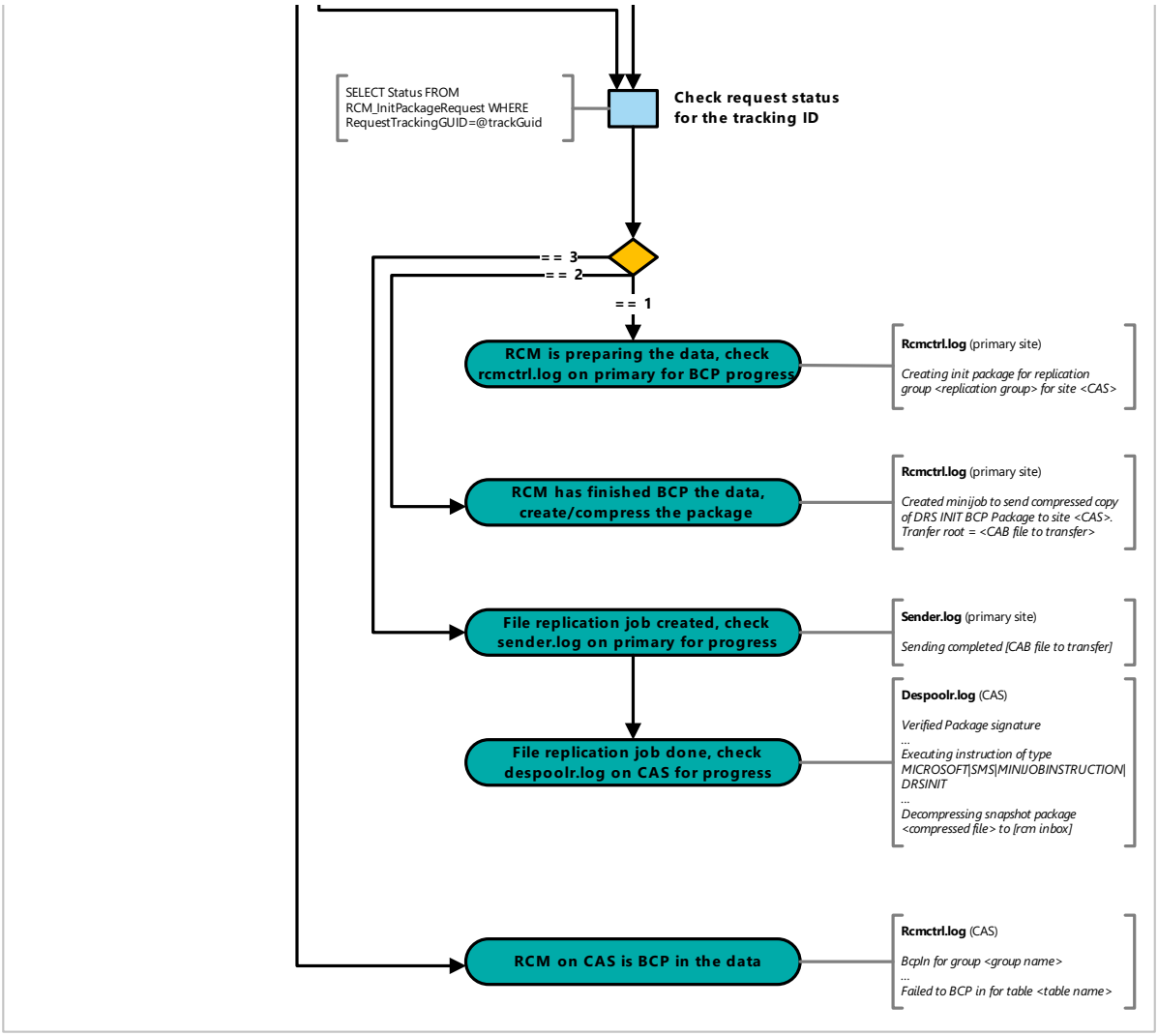
Troubleshoot site data reinit

9/11/2019 • 2 minutes to read • Edit Online

In a multi-site hierarchy, Configuration Manager uses SQL replication to transfer data between sites. For more information, see Database replication.

Use the following diagram to start troubleshooting SQL replication reinitialization (reinit) for site data in a Configuration Manager hierarchy:





Queries

This diagram uses the following queries:

Check if site replication hasn't finished reinit

```
SELECT * FROM RCM_DrsInitializationTracking dt
INNER JOIN ReplicationData rg
ON dt.ReplicationGroup = rg.ReplicationGroup
WHERE dt.InitializationStatus NOT IN (6,7)
AND rg.ReplicationPattern=N`Site'
```

Get the TrackingGuid & Status from the CAS

```
SELECT RequestTrackingGUID, InitializationStatus
FROM RCM_DrsInitializationTracking dt
INNER JOIN ReplicationData rg
ON dt.ReplicationGroup = rg.ReplicationGroup
WHERE dt.InitializationStatus NOT IN (6,7)
AND rg.ReplicationPattern=N'Site'
```

Get the TrackingGuid & Status from the primary site

```
SELECT RequestTrackingGUID, InitializationStatus
FROM RCM_DrsInitializationTracking dt
WHERE RequestTrackingGUID=@trackingGuid
```

Check primary site isn't in maintenance mode

```
SELECT * FROM ServerData
WHERE SiteStatus = 125
AND SiteCode=dbo.fnGetSiteCode()
AND ServerRole=N'Peer'
```

Check request status for the tracking ID

```
SELECT Status FROM RCM_InitPackageRequest
WHERE RequestTrackingGUID=@trackGuid
```

Next steps

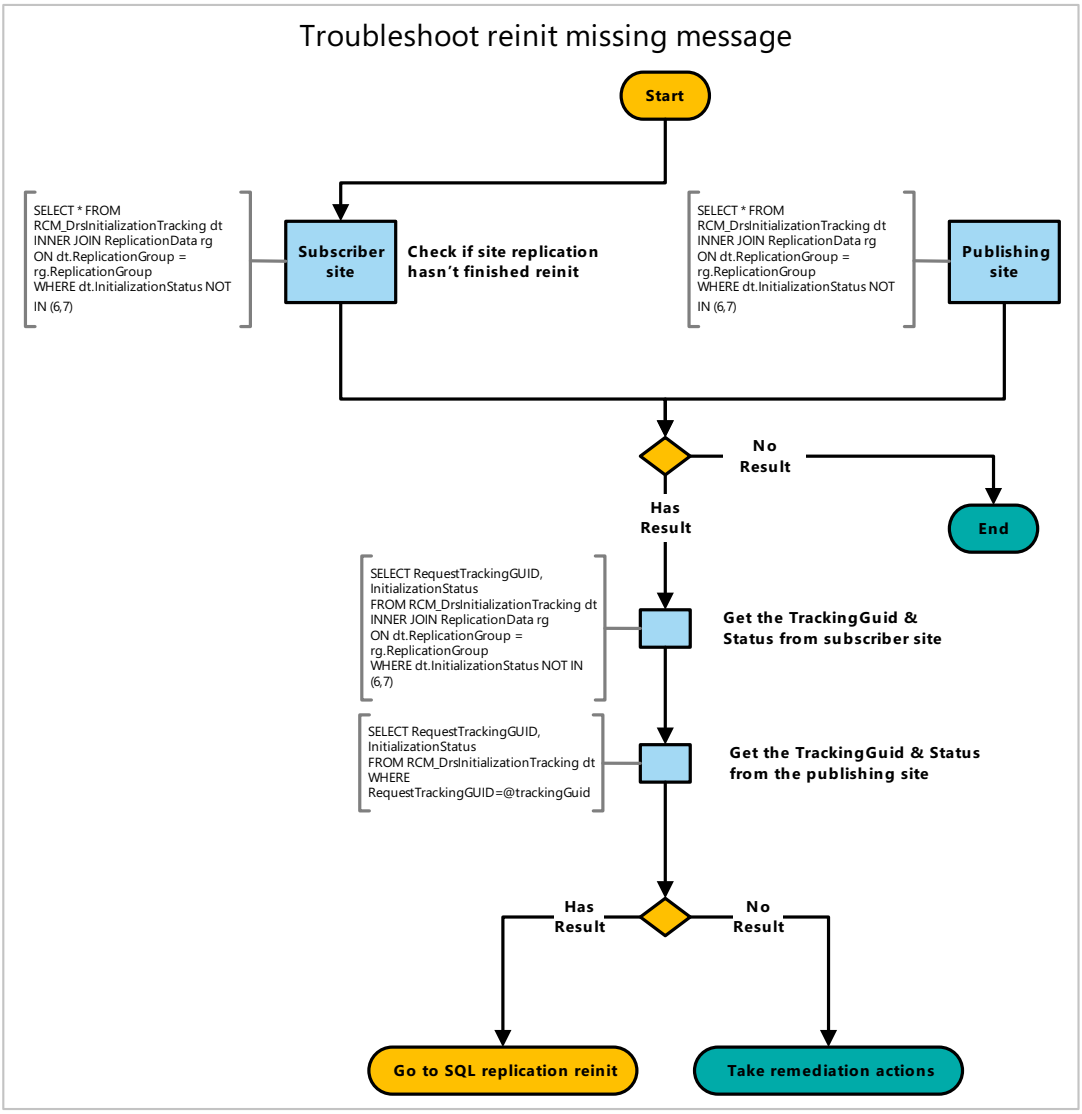
- Reinit missing message
- Global data reinit

Reinit missing message

8/12/2019 • 2 minutes to read • Edit Online

In a multi-site hierarchy, Configuration Manager uses SQL replication to transfer data between sites. For more information, see Database replication.

Use the following diagram to start troubleshooting a missing message with SQL replication reinitialization (reinit):



Queries

This diagram uses the following queries:

Check if site replication hasn't finished reinit

```
SELECT * FROM RCM_DrsInitializationTracking dt
INNER JOIN ReplicationData rg
ON dt.ReplicationGroup = rg.ReplicationGroup
WHERE dt.InitializationStatus NOT IN (6,7)
```

Get the TrackingGuid & Status from subscriber site

```
SELECT RequestTrackingGUID, InitializationStatus
FROM RCM_DrsInitializationTracking dt
INNER JOIN ReplicationData rg
ON dt.ReplicationGroup = rg.ReplicationGroup
WHERE dt.InitializationStatus NOT IN (6,7)
```

Get the TrackingGuid & Status from the publishing site

```
SELECT RequestTrackingGUID, InitializationStatus
FROM RCM_DrsInitializationTracking dt
WHERE RequestTrackingGUID=@trackingGuid
```

Remediation actions

Version 1902 and later

To detect the issue and reinit, run the Replication Link Analyzer.

Version 1810 and earlier

Run the following SQL query to get the `ReplicationGroupID`:

```
SELECT rd.ID AS ReplicationGroupID from ReplicationData rd
INNER JOIN RCM_DrsInitializationTracking it ON rd.ReplicationGroup = it.ReplicationGroup
WHERE it.RequestTrackingGUID=@trackingGuid
```

Then use the `InitializeData` method on the `SMS_ReplicationGroup` WMI class with the following values:

- ReplicationGroupID: from the SQL query above
- SiteCode1: parent site
- SiteCode2: child site

For more information, see InitializeData method in class SMS_ReplicationGroup.

Example

```
Invoke-WmiMethod –Namespace "root\sms\site_CAS" -Class SMS_ReplicationGroup –Name InitializeData -ArgumentList
"20", "CAS", "PR1"
```

Next steps

- SQL replication reinitialization (reinit)

Introduction to queries in System Center Configuration Manager

7/4/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can create and run queries to locate objects in a System Center Configuration Manager hierarchy that match your query criteria. These objects include items like specific types of computers or user groups. Queries can return most types of Configuration Manager objects, which include sites, collections, applications, and inventory data.

Query creation overview

When you create a query, you must specify a minimum of two parameters: where you want to search and what you want to search for. For example, to find the amount of hard drive space that's available on all computers in a Configuration Manager site, you can create a query to search the **Logical Disk** attribute class and the **Free Space (MB)** attribute for available hard drive space.

After you create an initial query, you can specify additional query criteria. For example, you can specify that the query results include only computers that are assigned to a specified site. You can also change how results are displayed so you can view the results in an order that's meaningful to you. For example, you can specify that the results are sorted by the amount of free hard drive space, in either ascending or descending order.

When you create a query, it's stored by Configuration Manager and displayed in the **Queries** node in the **Monitoring** workspace. From this location, you can create new queries and run, update, and manage existing queries.

You can also import a query into a query rule in a Configuration Manager collection. For more information, see How to create collections in System Center Configuration Manager.

Next steps

How to create queries in System Center Configuration Manager

How to manage queries in System Center Configuration Manager

7/4/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article can help you manage queries in System Center Configuration Manager.

For information about how to create queries, see How to create queries in System Center Configuration Manager.

Manage queries

In the **Monitoring** workspace, select **Queries**, select the query to manage, and then select a management task.

The following table provides information about the management tasks.

MANAGEMENT TASK	DETAILS
Run	Runs the selected query and displays the results in the Configuration Manager console.
Install Client	Opens the **Install Client Wizard**, which lets you install the Configuration Manager client on computers returned by the selected query. This option isn't available for queries that return mobile devices, users, or user groups. For more information about how to install Configuration Manager clients by using client push, see Deploy clients to Windows computers.
Export	Opens the **Export Objects Wizard**. This wizard lets you export the query to a Managed Object Format (MOF) file that you can then import at another site.
Move	Opens the **Move Selected Items** dialog box. This dialog box lets you move the selected query to a folder that you previously created under the **Queries** node.

Next steps

Create queries in System Center Configuration Manager

Create queries in System Center Configuration Manager

9/11/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article describes how to create and import queries in System Center Configuration Manager.

Create a query

Use this procedure to create a query in Configuration Manager.

1. In the Configuration Manager console, select **Monitoring**.
2. In the **Monitoring** workspace, select **Queries**. On the **Home** tab, in the **Create** group, select **Create Query**.
3. On the **General** tab of the **Create Query Wizard**, specify a unique name and, optionally, a comment for the query.
4. If you want to import an existing query to use as a basis for the new query, select **Import Query Statement**. In the **Browse Query** dialog box, select a query that you want to import, and then select **OK**.
5. In the **Object Type** list, select the type of object that you want the query to return. This table describes some examples of the types of objects you can search for:

OBJECT TYPE	DESCRIPTION
System Resource	Use to search for typical system attributes, like the NetBIOS name of a device, the client version, the client IP address, and Active Directory Domain Services information.
User Resource	Use to search for typical user information, like user names, user group names, and security group names.
Deployment	Use to search for typical attributes of a deployment, like the deployment name, the schedule, and the collection that it was deployed to.

6. Select **Edit Query Statement** to open the <Query Name> **Statement Properties** dialog box.
7. On the **General** tab of the <Query Name> **Statement Properties** dialog box, specify the attributes that the query returns and how they should be displayed. Select the **New** icon to add a new attribute. You can also select **Show Query Language** to enter or edit the query directly in WMI Query Language (WQL). For examples of WMI queries, see the Example WQL queries section in this article.

> **TIP**
> You can use the following reference documentation to help you construct your own WQL queries:
>
> - WQL (SQL for WMI)
> - WHERE Clause
> - WQL Operators

8. On the **Criteria** tab of the <Query Name> **Statement Properties** dialog box, specify criteria that are used to refine the results of the query. For example, you could return only resources that have a site code of **XYZ**. You can configure multiple criteria for a query.

> **IMPORTANT**
> If you create a query that contains no criteria, the query will return all devices in the **All Systems** collection.

9. On the **Joins** tab of the <Query Name> **Statement Properties** dialog box, you can combine data from two different attributes into your query results. Although Configuration Manager automatically creates query joins when you choose different attributes for your query result, the **Joins** tab provides more advanced options. Configuration Manager supports these attribute classes:

JOIN TYPE	DESCRIPTION
Inner	Displays only matching results. Always used by joins that are created automatically.
Left	Displays all results for the base attribute and only the matching results for the join attribute.
Right	Displays all results for the join attribute and only the matching results for the base attribute.
Full	Displays all results for both the base attribute and the join attribute.

   For more information about how to use join operations, see the SQL Server documentation.

10. Select **OK** to close the <Query Name> **Statement Properties** dialog box.
11. On the **General** tab of the **Create Query Wizard**, specify that the results of the query aren't limited to the members of a collection, that they are limited to the members of a specified collection, or that a prompt for a collection appears each time the query is run.
12. Complete the wizard to create the query. The new query appears in the **Queries** node in the **Monitoring** workspace.

Import a query

Use this procedure to import a query into Configuration Manager. For information about how to export queries, see How to manage queries in System Center Configuration Manager.

1. In the Configuration Manager console, select **Monitoring**.
2. In the **Monitoring** workspace, select **Queries**. On the **Home** tab, in the **Create** group, select **Import Objects**.

3. On the **MOF File Name** page of the **Import Objects Wizard**, select **Browse** to select the Managed Object Format (MOF) file that contains the query that you want to import.

4. Review the information about the query to be imported and then complete the wizard. The new query appears on the **Queries** node in the **Monitoring** workspace.

Example WQL queries

This section contains example WQL queries that you can use in your hierarchy or modify for other purposes. To use these queries, select **Show Query Language** in the **Query Statement Properties** dialog box. Then copy and paste the query into the **Query Statement** field.

> **TIP**
> Use the wildcard character `%` to signify any string of characters. For example, `%Visio%` returns Microsoft Office Visio 2010.

Computers that run Windows 7

Use the following query to return the NetBIOS name and operating system version of all computers that run Windows 7.

> **TIP**
> To return computers that run Windows Server 2008 R2, change `%Workstation 6.1%` to `%Server 6.1%`.

```
select SMS_R_System.NetbiosName,
SMS_R_System.OperatingSystemNameandVersion from
SMS_R_System where
SMS_R_System.OperatingSystemNameandVersion like "%Workstation 6.1%"
```

Computers with a specific software package installed

Use the following query to return the NetBIOS name and software package name of all computers that have a specific software package installed. This example returns all computers with a version of Microsoft Visio installed. Replace `Microsoft%Visio%` with the software package that you want to query for.

> **TIP**
> This query searches for the software package by using the names that are displayed in the programs list in Windows Control Panel.

```
select SMS_R_System.NetbiosName,
SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName from
SMS_R_System inner join SMS_G_System_ADD_REMOVE_PROGRAMS on
SMS_G_System_ADD_REMOVE_PROGRAMS.ResourceId =
SMS_R_System.ResourceId where
SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName like "Microsoft%Visio%"
```

Computers in a specific Active Directory Domain Services organizational unit

Use the following query to return the NetBIOS name and organizational unit (OU) name of all computers in a specified OU. Replace the text `OU Name` with the name of the OU that you want to query for.

```
select SMS_R_System.NetbiosName,
SMS_R_System.SystemOUName from
SMS_R_System where
SMS_R_System.SystemOUName = "OU Name"
```

Computers with a specific NetBIOS name

Use the following query to return the NetBIOS name of all computers that begin with a specific string of characters. In this example, the query returns all computers with a NetBIOS name that begins with `ABC`.

```
select SMS_R_System.NetbiosName from
SMS_R_System where SMS_R_System.NetbiosName like "ABC%"
```

Devices of a specific type

Device types are stored in the Configuration Manager database under the resource class **sms_r_system** and the attribute name **AgentEdition**. Use this query to retrieve only the devices that match the agent edition of the device type that you specify:

```
Select SMS_R_System.ClientEdition from SMS_R_System where SMS_R_System.ClientEdition = <Device ID>
```

Use one of these values for <Device ID>:

DEVICE TYPE	VALUE OF AGENTEDITION
Windows desktop or laptop computer	0
Windows ARM-based device (running Windows RT)	1
Windows Mobile 6.5	2
Nokia Symbian	3
Windows Phone	4
Mac computer	5
Windows CE	6
Windows Embedded	7
iOS	8
iPad	9
iPod touch	10
Android	11
Intel system on a chip	12
Unix and Linux servers	13

DEVICE TYPE	VALUE OF AGENTEDITION
Apple macOS (MDM)	14
Microsoft HoloLens (MDM)	15
Microsoft Surface Hub (MDM)	16
Android for Work	17

For example, if you want to return only Mac computers, use this query:

```
Select SMS_R_System.ClientEdition from SMS_R_System where SMS_R_System.ClientEdition = 5
```

Next steps

How to manage queries

Security and privacy for queries in System Center Configuration Manager

7/4/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Queries in System Center Configuration Manager let you retrieve information from the site database according to criteria that you specify. Configuration Manager collects site database information during standard operation. For example, by using information that's been collected during discovery or inventory, you can configure a query to identify devices that meet specified criteria.

For more information about queries, see Introduction to queries in System Center Configuration Manager. For security best practices and privacy information about Configuration Manager operations that collect the data you can retrieve by using queries, see Security and privacy for System Center Configuration Manager.

Security best practices for queries

Use this security best practice for queries.

SECURITY BEST PRACTICE	MORE INFORMATION
When you export or import a query that's saved to a network location, secure the location and the network channel.	Restrict who can access the network folder. Use Server Message Block (SMB) signing or Internet Protocol security (IPsec) between the network location and the site server to prevent an attacker from tampering with the query data before it's imported.

Next steps

Security and privacy for System Center Configuration Manager

Introduction to reporting in System Center Configuration Manager

9/5/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Reporting in System Center Configuration Manager provides a set of tools and resources that help you use the advanced reporting capabilities of SQL Server Reporting Services (SSRS) and the rich authoring experience that Reporting Services Report Builder provides. Reporting helps you gather, organize, and present information about users, hardware and software inventory, software updates, applications, site status, and other Configuration Manager operations in your organization. Reporting provides you with a number of predefined reports that you can use without changes, or that you can modify to meet your requirements, and you can create custom reports. Use the following sections to help you manage reporting in Configuration Manager.

SQL Server Reporting Services

SQL Server Reporting Services provides a full range of ready-to-use tools and services to help you create, deploy, and manage reports for your organization and programming features that enable you to extend and customize your reporting functionality. Reporting Services is a server-based reporting platform that provides comprehensive reporting functionality for a variety of data sources.

Configuration Manager uses SQL Server Reporting Services as its reporting solution. Integration with Reporting Services provides the following advantages:

- Uses an industry standard reporting system to query the Configuration Manager database.
- Displays reports by using the Configuration Manager Report Viewer or by using Report Manager, which is a web-based connection to the report.
- Provides high performance, availability, and scalability.
- Provides subscriptions to reports that users can subscribe to; for example, a manager could subscribe to automatically receive an emailed report each day that details the status of a software update rollout.
- Exports reports that users can select in a variety of popular formats.

  For more information about Reporting Services, see SQL Server Reporting Services in the SQL Server 2008 Books Online.

Reporting Services Point

The reporting services point is a site system role that is installed on a server that is running Microsoft SQL Server Reporting Services. The reporting services point copies the Configuration Manager report definitions to Reporting Services, creates report folders based on report categories, and sets security policy on the report folders and reports based on the role-based permissions for Configuration Manager administrative users. In a 10-minute interval, the reporting services point connects to Reporting Services to reapply the security policy if it has been changed, for example, by using Report Manager. For more information about how to plan for and install a reporting services point, see the following documentation:

- Planning for reporting in System Center Configuration Manager
- Configuring reporting in System Center Configuration Manager

Configuration Manager reports

Configuration Manager provides report definitions for over 400 reports in over 50 report folders, which are copied to the root report folder in SQL Server Reporting Services during the reporting services point installation process. The reports are displayed in the Configuration Manager console and organized in subfolders based on the report category. Reports are not propagated up or down the Configuration Manager hierarchy; they run only against the database of the site in which they are created. However, because Configuration Manager replicates global data throughout the hierarchy, you have access to hierarchy-wide information. When a report retrieves data from a site database, it has access to site data for the current site and child sites, and global data for every site in the hierarchy. Like other Configuration Manager objects, an administrative user must have the appropriate permissions to run or modify reports. To run a report, an administrative user must have the **Run Report** permission for the object. To create or modify a report, an administrative user must have the **Modify Report** permission for the object.

Creating and modifying reports

Configuration Manager uses Microsoft SQL Server Report Builder as the exclusive authoring and editing tool for model-based and SQL-based reports. When you create or edit a report in the Configuration Manager console, Report Builder opens. For more information about managing reports, see the Operations and maintenance for reporting in System Center Configuration Manager.

Running reports

When you run a report in the Configuration Manager console, Report Viewer opens and connects to Reporting Services. After you specify any required report parameters, Reporting Services then retrieves the data and displays the results in the viewer. You can also connect to the SQL Services Reporting Services, connect to the data source for the site, and run reports.

Report prompts

A report prompt or report parameter in Configuration Manager is a report property that you can configure when a report is created or modified. Report prompts are created to limit or target the data that a report retrieves. A report can contain more than one prompt as long as the prompt names are unique and contain only alphanumeric characters that conform to the SQL Server rules for identifiers.

When you run a report, the prompt requests a value for a required parameter and, based on the value, retrieves the report data. For example, the **Computer information for a specific computer** report retrieves the computer information for a specific computer and prompts the administrative user for a computer name. Reporting Services passes the specified value to a variable that is defined in the SQL statement for the report.

Report links

Report links in Configuration Manager are used in a source report to provide administrative users with easy access to additional data, such as more detailed information about each of the items in the source report. If the destination report requires one or more prompts to run, the source report must contain a column with the appropriate values for each prompt. You must specify the column number that provides the value for the prompt. For example, you might link a report that lists computers that were discovered recently to a report that lists the last messages that were received for a specific computer. When the link is created, you might specify that column 2 in the source report contains computer names, which is a required prompt for the destination report. When the source report is run, link icons appear to the left of each row of data. When you click the icon on a row, Report Viewer passes the value in the specified column for that row as the prompt value that is required to display the destination report. A report can be configured with only one link, and that link can connect only to a single destination resource.

WARNING

If you move a destination report to a different report folder, the location for the destination report changes. The report link in the source report is not automatically updated with the new location, and the report link will not work in the source report.

Report folders

Report folders in System Center Configuration Manager provide a method to sort and filter reports that are stored in Reporting Services. Report folders are particularly useful when you have many reports to manage. When you install a reporting services point, reports are copied to Reporting Services and organized into more than 50 report folders. The report folders are read-only. You cannot modify them in the Configuration Manager console.

Report subscriptions

A report subscription in Reporting Services is a recurring request to deliver a report at a specific time or in response to an event, and in an application file format that you specify in the subscription. Subscriptions provide an alternative to running a report on demand. On-demand reporting requires that you actively select the report each time you want to view the report. In contrast, subscriptions can be used to schedule and then automate the delivery of a report.

You can manage report subscriptions in the Configuration Manager console. They are processed on the report server. The subscriptions are distributed by using delivery extensions that are deployed on the server. By default, you can create subscriptions that send reports to a shared folder or to an email address. For more information about managing report subscriptions, see Operations and maintenance for reporting in System Center Configuration Manager.

Report Builder

Configuration Manager uses Microsoft SQL Server Reporting Services Report Builder as the exclusive authoring and editing tool for both model-based and SQL-based reports. When you initiate the action to create or edit a report in the Configuration Manager console, Report Builder opens. When you create or modify a report for the first time, Report Builder is installed automatically. The version of Report Builder associated with the installed version of SQL Server opens when you run or edit reports.

The Report Builder installation adds support for over 20 languages. When you run Report Builder, it displays data in the language of the operating system that is running on the local computer. If Report Builder does not support the language, the data is displayed in English. Report Builder supports the full capabilities of SQL Server 2008 Reporting Services, which includes the following capabilities:

- Delivers an intuitive report authoring environment with an appearance similar to Microsoft Office.
- Offers the flexible report layout of SQL Server 2008 Report Definition Language (RDL).
- Provides various forms of data visualization including charts and gauges.
- Provides richly formatted text boxes.
- Exports to Microsoft Word format.

  You can also open Report Builder from SQL Server Reporting Services.

Report models in SQL Server Reporting Services

SQL Reporting Services in Configuration Manager uses report models to help administrative users select items

from the database to include in model-based reports. For the administrative user who is building the report, report models expose only specified views and items to choose from. To create model-based reports, at least one report model has to be available. Report models have the following features:

- You can give database fields and views logical business names to facilitate producing reports. Knowledge of the database structure is not required to produce reports.
- You can group items logically.
- You can define relationships between items.
- You can secure model elements so that administrative users can see only the data that they have permission to see.

  Although Configuration Manager provides sample report models, you can also define report models to meet your own business requirements. For more information about how to create report models, see Creating custom report models for System Center Configuration Manager in SQL Server Reporting Services.

Next steps

Planning for reporting

Planning for reporting in System Center Configuration Manager

2/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Reporting in System Center Configuration Manager provides a set of tools and resources that help you use the advanced reporting capabilities of SQL Server Reporting Services. Use the following sections to help you plan for reporting in Configuration Manager.

Determine where to install the Reporting Services Point

When you run Configuration Manager reports at a site, the reports have access to the information in the site database in which it connects. Use the following sections to help you determine where to install the reporting services point and what data source to use.

> **NOTE**
> For more information about planning for site systems in Configuration Manager, see Add site system roles.

Supported site system servers

You can install the reporting services point on a central administration site and primary sites, and on multiple site systems at a site and at other sites in the hierarchy. The reporting services point is not supported on secondary sites. The first reporting services point at a site is configured as the default report server. You can add more reporting services points at a site, but the default report server at each site is actively used for Configuration Manager reports. You can install the reporting services point on the site server or a remote site system. However, as a best practice for performance reasons, use Reporting Services on a remote site system server.

Data replication considerations

Configuration Manager classifies the data that it replicates as either global data or site data. Global data refers to objects that were created by administrative users and that are replicated to all sites throughout the hierarchy, while secondary sites receive only a subset of global data. Examples of global data include software deployments, software updates, collections, and role-based administration security scopes. Site data refers to operational information that Configuration Manager primary sites and the clients that report to primary sites create. Site data replicates to the central administration site but not to other primary sites. Examples of site data include hardware inventory data, status messages, alerts, and the results from query-based collections. Site data is only visible at the central administration site and the primary site where the data originates.

Consider the following factors to help you determine where to install your reporting services points:

- A reporting services point with the central administration site database as its reporting data source has access to all global and site data in the Configuration Manager hierarchy. If you require reports that contain site data for multiple sites in a hierarchy, consider installing the reporting services point on a site system at the central administration site and use the central administration site's database as the reporting data source.

- A reporting services point with the child primary site database as its reporting data source has access to global data and site data for only the local primary site and any child secondary sites. Site data for other primary sites in the Configuration Manager hierarchy is not replicated to the primary site, and therefore Reporting Services cannot access it. If you require reports that contain site data for a specific primary site or

global data, but you do not want the report user to have access to site data from other primary sites, install a reporting services point on a site system at the primary site and use the primary site's database as the reporting data source.

Network bandwidth considerations

Site system servers in the same site communicate with each other by using server message block (SMB), HTTP, or HTTPS, depending on how you configure the site. Because these communications are unmanaged and can occur at any time without network bandwidth control, review your available network bandwidth before you install the reporting services point role on a site system.

> **NOTE**
> For more information about planning for site systems, see Add site system roles.

Planning for role-based administration for reports

Security for reporting is much like other objects in Configuration Manager where you can assign security roles and permissions to administrative users. Administrative users can only run and modify reports for which they have appropriate security rights. To run reports in the Configuration Manager console, you must have the **Read** right for the **Site** permission and the permissions configured for specific objects.

However, unlike other objects in Configuration Manager, the security rights that you set for administrative users in the Configuration Manager console must also be configured in Reporting Services. When you configure security rights in the Configuration Manager console, the reporting services point connects to Reporting Services and sets appropriate permissions for reports. For example, the **Software Update Manager** security role has the **Run Report** and **Modify Report** permissions associated with it. Administrative users who are only assigned the **Software Update Manager** role can only run and modify reports for software updates. Reports for other objects are not displayed in the Configuration Manager console. The exception to this is that some reports are not associated with specific Configuration Manager securable objects. For these reports, the administrative user must have the **Read** right for the **Site** permission to run the reports and the **Modify** right for the **Site** permission to modify the reports.

Reports are fully enabled for role-based administration. The data for all reports included with Configuration Manager is filtered based on the permissions of the administrative user who runs the report. Administrative users with specific roles can only view information defined for their roles.

For more information about security rights for reporting, see Configure reporting.

For more information about role-based administration in Configuration Manager, see Configure role-based administration.

Next steps

Use the following additional topics to help you plan for reporting in Configuration Manager:

- Prerequisites for reporting in System Center Configuration Manager
- Best practices for reporting in System Center Configuration Manager

Prerequisites for reporting in System Center Configuration Manager

9/5/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Reporting in System Center Configuration Manager has external dependencies and dependencies within the product.

Dependencies external to Configuration Manager

The following table lists the external dependencies for reporting.

PREREQUISITE	MORE INFORMATION
SQL Server Reporting Services	Before you can use reporting in Configuration Manager, you must install and configure SQL Server Reporting Services. For information about planning and deploying Reporting Services in your environment, see the Reporting Services section in the SQL Server 2008 Books Online.
Site system role dependencies for the computers that run the reporting services point.	Supported configurations for System Center Configuration Manager

Dependencies internal to Configuration Manager

The following table lists the dependencies for reporting in Configuration Manager.

PREREQUISITE	MORE INFORMATION
Reporting services point	The reporting services point site system role must be configured before you can use reporting in Configuration Manager. For more information about how to install and configure a reporting services point, see Configuring reporting in System Center Configuration Manager.

Supported SQL Server versions for the Reporting Services Point

The Reporting Services database can be installed on either the default instance or a named instance of a 64-bit SQL Server installation. The SQL Server instance can be co-located with the site system server, or on a remote computer.

The following table lists the SQL Server versions that are supported by the reporting services point.

SQL SERVER VERSION	REPORTING SERVICES POINT
SQL Server 2017 with a minimum of cumulative update 2 - Standard - Enterprise	Yes, starting in Configuration Manager version 1710

SQL SERVER VERSION	REPORTING SERVICES POINT
SQL Server 2016 with SP1 - Standard - Enterprise	Yes
SQL Server 2016 - Standard - Enterprise	Yes
SQL Server 2014 with SP2 - Standard - Enterprise	Yes
SQL Server 2014 with SP1 - Standard - Enterprise	Yes
SQL Server 2012 with SP4 - Standard - Enterprise	Yes
SQL Server 2012 with SP3 - Standard - Enterprise	Yes
SQL Server 2008 R2 with SP3 - Standard - Enterprise - Datacenter	Yes, for supported versions of Configuration Manager prior to 1702.
SQL Server Express 2008 R2 with SP3	Not Supported

Next steps

Operations and maintenance for reporting

Best practices for reporting in System Center Configuration Manager

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the following best practices for reporting in System Center Configuration Manager:

For best performance, install the reporting services point on a remote site system server

Although you can install the reporting services point on the site server or a remote site system, performance is increased when you install the reporting services point on a remote site system server.

Optimize SQL Server Reporting Services queries

Typically, any reporting delays are because of the time it takes to run queries and retrieve the results. If you are using Microsoft SQL Server, tools such as Query Analyzer and Profiler can help you optimize queries.

Schedule report subscription processing to run outside standard office hours

Whenever possible, schedule report subscription processing to run outside normal office standard hours to minimize the CPU processing on the Configuration Manager site database server. This practice also improves availability for unpredicted report requests.

Next steps

Configure reporting

List of reports in Configuration Manager

2/28/2019 • 61 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager supplies many built-in reports covering many of the reporting tasks that you might want to do. You can also use the SQL statements in these reports to help you to write your own reports.

The following reports are included with Configuration Manager. The reports appear in various categories.

Administrative security

The following six reports are listed under the **Administrative Security** category.

REPORT NAME	DESCRIPTION
Administration activity log	Displays a record of administrative changes made for administrative users, security roles, security scopes, and collections.
Administrative users security assignments	Displays administrative users, their associated security roles, and the security scopes associated with each security role for each user.
Objects secured by a single security scope	Displays objects that an administrator assigned to only the specified security scope. This report doesn't display objects that an administrator associates with more than one security scope.
Security for a specific or multiple Configuration Manager objects	Displays securable objects, the security scopes associated with the objects, and which administrative users have rights to the objects.
Security roles summary	Displays security roles and the Configuration Manager administrators associated with each role.
Security scopes summary	Displays security scopes and the Configuration Manager administrative users and security groups associated with each scope.

Alerts

The following two reports are listed under the **Alerts** category.

REPORT NAME	DESCRIPTION
Alert scorecard	Displays a summary of all postponed alerts that were generated between the specified start and finish date.
Alerts Generated Most Often	Displays a summary of the alerts that were generated most often from today back to the specified date for the specified feature area.

Asset Intelligence

The following 67 reports are listed under the **Asset Intelligence** category.

REPORT NAME	DESCRIPTION
Hardware 01A - Summary of computers in a specific collection	Displays an Asset Intelligence summary view of computers in a collection you specify.
Hardware 03A - Primary computer users	Displays users and the count of computers on which they're the primary user.
Hardware 03B - Computers for a specific primary console user	Displays all computers for which a specified user is the primary console user.
Hardware 04A - Computers with multiple users (shared)	Displays computers that don't have a primary user because no one user has a signed-in time greater than 66%.
Hardware 05A - Console users on a specific computer	Displays all of the console users on a specified computer.
Hardware 06A - Computers for which console users could not be determined	Helps administrative users identify computers that need to have security logging turned on.
Hardware 07A - USB devices by manufacturer	Displays USB devices, grouped by manufacturer.
Hardware 07B - USB devices by manufacturer and description	Displays USB devices, grouped by manufacturer and description.
Hardware 07C - Computers with a specific USB device	Displays all the computers with a specified USB device.
Hardware 07D - USB devices on a specific computer	Displays all USB devices on a specified computer.
Hardware 08A - Hardware that is not ready for a software upgrade	Displays hardware that doesn't meet the minimum hardware requirements.
Hardware 09A - Search for computers	Displays a summary of computers matching keyword filters. These filters are computer name, Configuration Manager site, domain, top console user, operating system, manufacturer, or model.
Hardware 10A - Computers in a specified collection that have changed during a specified timeframe	Displays a list of computers in a specified collection where a hardware class has changed during a specified time period.
Hardware 10B - Changes on a specified computer within a specified timeframe	Displays the classes that have changed on a specified computer within a specified time period.
License 01A - Microsoft Volume License ledger for Microsoft license statements	Displays an inventory of all Microsoft software titles that are available from the Microsoft Volume Licensing program.
License 01B - Microsoft Volume License ledger item by sales channel	Identifies and displays sales channel for inventoried Microsoft Volume License software.
License 01C - Computers with a specific Microsoft Volume License ledger item and sales channel	Identifies and displays computers that have a specified item from the Microsoft Volume license ledger.

REPORT NAME	DESCRIPTION
License 01D - Microsoft Volume License ledger products on a specific computer	Identifies and displays all Microsoft Volume license ledger items on a specified computer.
License 02A - Count of licenses nearing expiration by time ranges	Displays a count of licenses nearing expiration by a specified time range. The displayed products have their licenses managed by the Software Licensing Service.
License 02B - Computers with licenses nearing expiration	Displays the specified computers with licenses that are nearing expiration.
License 02C - License information on a specific computer	Displays products on a specified computer that have their licenses managed by the Software Licensing Service.
License 03A - Count of licenses by license status	Displays products, by license status, which have their licenses managed by the Software Licensing Service.
License 03B - Computers with a specific license status	Displays products, with a specified license status, whose licenses are managed by the Software Licensing Service.
License 04A - Count of products managed by software licensing	Displays a count of products that have their licenses managed by the Software Licensing Service.
License 04B - Computers with a specific product managed by Software Licensing Service	Displays computers, managed by the Software Licensing Service, that include a specified product.
License 05A - Computers providing Key Management Service	Displays computers that act as Key Management Servers.
License 06A - Processor counts for per-processor licensed products	Displays the number of processors on computers using Microsoft products that support per-processor licensing.
License 06B - Computers with a specific product that supports per-processor licensing	Displays a list of computers where a specified Microsoft product that supports per-processor licensing is installed.
License 14A - Microsoft Volume Licensing reconciliation report	Displays reconciliation on software licenses acquired through Microsoft Volume License Agreement and the actual inventory count.
License 14B - List of Microsoft software inventory not found in MVLS	This report displays Microsoft software titles in use that aren't found in the Microsoft Volume License Agreement.
License 15A - General license reconciliation report	Displays reconciliation on general software licenses acquired and the actual inventory count.
License 15B - General license reconciliation report by computer	Displays computers that installed the licensed product with a specified version.
Software 01A - Summary of installed software in a specific collection	Displays a summary of installed software ordered by the number of instances found from inventory.
Software 02A - Product families for a specific collection	Displays the product families and the count of software in the family for a specified collection.

REPORT NAME	DESCRIPTION
Software 02B - Product categories for a specific product family	Displays the product categories in a specified product family and the count of software within the category.
Software 02C - Software in a specific product family and category	Displays all software that is in the specified product family and category.
Software 02D - Computers with specific software installed	Displays all computers with specified software installed.
Software 02E - Installed software on a specific computer	Displays all software installed on a specified computer.
Software 03A - Uncategorized software	Displays the software that is either categorized as unknown or has no categorization.
Software 04A - Software configured to automatically run on computers	Displays a list of software configured to automatically run on computers.
Software 04B - Computers with specific software configured to automatically run	Displays all computers with specified software configured to automatically run.
Software 04C - Software configured to automatically run on a specific computer	Displays installed software configured to automatically run on a specified computer.
Software 05A - Browser Helper Objects	Displays the browser helper objects installed on computers in a specified collection.
Software 05B - Computers with a specific Browser Helper Object	Displays all of the computers with a specified browser helper object.
Software 05C - Browser Helper Objects on a specific computer	Displays all browser helper objects on the specified computer.
Software 06A - Search for installed software	This report provides a summary of installed software. It searches based on the following criteria: product name, publisher, or version.
Software 06B - Software by product name	Displays a summary of installed software based on a specified product name.
Software 07A - Recently used executable programs by the count of computers	Displays executable programs that users recently used. It also includes the count of computers on which users used the program. Software metering must be enabled for this site to view this report.
Software 07B - Computers that recently used a specified executable program	Displays the computers on which users recently used a specified executable program. This report requires that you enable the software metering client setting.
Software 07C - Recently used executable programs on a specified computer	Displays executable files that users recently used on a specified computer. This report requires that you enable the software metering client setting.

REPORT NAME	DESCRIPTION
Software 08A - Recently used executable programs by the count of users	Displays executable programs that users recently used. It also includes a count of users that most recently used the program. This report requires that you enable the software metering client setting.
Software 08B - Users that recently used a specified executable program	Displays the users that most recently used a specified executable program. This report requires that you enable the software metering client setting.
Software 08C - Recently used executable programs by a specified user	Displays executable programs that the specified user used recently. This report requires that you enable the software metering client setting.
Software 09A - Infrequently used software	Displays software titles that users haven't used during a specified period of time.
Software 09B - Computers with infrequently used software installed	Displays computers with installed software that users haven't used for a specified period of time. The specified period of time is based on the value specified in the 'Software 09A - Infrequently used software' report.
Software 10A - Software titles with specific multiple custom labels defined	Displays software titles based on matching of all specified custom label criteria. Up to three custom labels can be selected to refine a software title search.
Software 10B - Computers with a specific custom-labeled software title installed	Displays all computers in this collection that have the specified custom-labeled software title installed.
Software 11A - Software titles with a specific custom label defined	Displays software titles based on matching of at least one of the specified custom label criteria.
Software 12A - Software titles without a custom label	Displays all software titles that don't have a custom label defined.
Software 14A - Search for software identification tag enabled software	Displays a count of installed software with a software identification tag enabled.
Software 14B - Computers with specific software identification tag enabled software installed	Displays all computers that have installed software with a specified software identification tag enabled.
Software 14C - Installed software identification tag enabled software on a specific computer	Displays all installed software with a specified software identification tag enabled on a specified computer.
Lifecycle 01A - Computers with a specific software product	View a list of computers on which a specified product is detected.
Lifecycle 02A - List of machines with expired products in the organization	View computers that have expired products on them. You can filter this report by product name.
Lifecycle 03A - List of expired products found in the organization	View details for products in your environment that have expired lifecycle dates.
Lifecycle 04A - General Product Lifecycle overview	View a list of product lifecycles. Filter the list by product name and days to expiration.

REPORT NAME	DESCRIPTION
Lifecycle 05A - Product lifecycle dashboard	Starting in version 1810, this report includes similar information as the in-console dashboard.

Client push

The following four reports are listed under the **Client Push** category.

REPORT NAME	DESCRIPTION
Client push installation status details	Displays information about the client push installation process for all sites.
Client push installation status details for a specified site	Displays information about the client push installation process for a specified site.
Client push installation status summary	Displays a summary view of the client push installation status for all sites.
Client push installation status summary for a specified site	Displays a summary view of the client push installation status for a specified site.

Client status

The following seven reports are listed under the **Client Status** category.

REPORT NAME	DESCRIPTION
Client remediation details	Displays details of client remediation actions for a collection you specify.
Client remediation summary	Displays a summary of client remediation actions for a specified collection.
Client status history	Displays a historical view of overall client status in the site.
Client status summary	Displays the client check results of active clients for a given collection.
Client time to request policy	Displays the percentage of clients that requested policy at least once in the last 30 days. Each day represents a percentage of total clients that requested policy since the first day in the cycle.
Clients with failed client check details	Displays details about clients that client check failed for a specified collection.
Inactive clients details	Displays a detailed list of inactive clients for a given collection.

Company resource access

The following three reports are listed under the **Company Resource Access** category.

REPORT NAME	DESCRIPTION
Certificate issuance history	Displays the history of certificates issued by the certificate registration point to users and devices for the specified date range.
List of assets by certificate issuance status	Displays the devices or users in a specified certificate issuance state following the evaluation of a specified certificate profile.
List of assets with certificates nearing expiry	Displays the devices or users with certificates that expire on or before the specified date.

Compliance and settings management

The following 22 reports are listed under the **Compliance and Settings Management** category.

REPORT NAME	DESCRIPTION
Compliance history of a configuration baseline	Displays the history of the changes in compliance of a configuration baseline for the specified date range.
Compliance history of a configuration item	Displays the history of the changes in compliance of a configuration item for the specified date range.
Conditional Access Compliance for User	Displays detailed conditional access compliance for a specific user.
Conditional Access Compliance Report	A conditional access compliance report for each targeted compliance policy.
Details of compliant rules of configuration items in a configuration baseline for an asset	Displays information about the rules evaluated as compliant for a specified configuration item for a specified device or user.
Details of conflicting rules of configuration items in a configuration baseline for an asset	Displays information about rules in a deployed configuration item that conflict with other rules. Include the other rules in the same or another deployed configuration item.
Details of errors of configuration items in a configuration baseline for an asset	Displays information about errors generated by a specified configuration item for a specified device or user.
Details of non-compliant rules of configuration items in a configuration baseline for an asset	Displays information about rules that were evaluated as noncompliant for a specified configuration item, for a specified device or user.
Details of remediated rules of configuration items in a configuration baseline for an asset	Displays information about rules that were remediated by a specified configuration item for a specified device or user.
List of assets by compliance state for a configuration baseline	Displays the devices or users in a specified compliance state following the evaluation of a specified configuration baseline.
List of assets by compliance state for a configuration item in a configuration baseline	Displays the devices or users in a specified compliance state following the evaluation of a specified configuration item.
List of noncompliant Apps and Devices for a specified user	Displays information about users and devices that have apps installed that aren't compliant with a policy you specified.

REPORT NAME	DESCRIPTION
List of rules conflicting with a specified rule for an asset	Displays a list of rules that conflict with a specified rule for a deployed configuration item.
List of unknown assets for a configuration baseline	Displays a list of devices or users that haven't yet reported any compliance data for a specified configuration baseline.
List of unknown assets for a configuration item	Displays a list of devices or users that haven't yet reported any compliance data for a specified configuration item.
Rules and errors summary of configuration items in a configuration baseline for an asset	Displays a summary of the compliance state of the rules and any setting errors for a specified configuration item. The configuration item must be deployed to a device or user.
Summary compliance by configuration baseline	Displays a summary of the overall compliance of deployed configuration baselines in the hierarchy.
Summary compliance by configuration items for a configuration baseline	Displays a summary of the compliance of configuration items in a specified configuration baseline.
Summary compliance by configuration policies	Displays a summary of the compliance of configuration policies.
Summary compliance of a configuration baseline for a collection	Displays a summary of the overall compliance of a specified configuration baseline. The configuration item must be deployed to the specified collection.
Summary of Users who have Noncompliant Apps	Displays information about users that have apps installed that aren't compliant with a policy you specified.
Terms and Conditions acceptance	Displays Terms and Conditions items and which version each user has accepted.

Data warehouse

The following seven reports are listed under the **Data warehouse** category.

REPORT NAME	DESCRIPTION
Application Deployment	Historical: View details for application deployment for a specific application and machine.
Endpoint Protection and Software Update Compliance	Historical: View computers that are missing software updates.
General Hardware Inventory	Historical: View all hardware inventory for a specific machine.
General Software Inventory	Historical: View all software inventory for a specific machine.
Infrastructure Health Overview	Historical: Displays an overview of the health of your Configuration Manager infrastructure.
List of Malware Detected	Historical: View malware that has been detected in the organization.

REPORT NAME	DESCRIPTION
Software Distribution Summary	Historical: A summary of software distribution for a specific advertisement and machine.

Device management

The following 37 reports are listed under the **Device Management** category.

REPORT NAME	DESCRIPTION
All corporate-owned mobile devices	Displays all corporate owned mobile devices.
All mobile device clients	Displays information about all mobile device clients. Devices that are managed by the Exchange Server connector aren't included.
Certificate issues on mobile devices that are managed by the Configuration Manager client for Windows CE and that are not healthy	Displays detailed information about certificate issues on mobile devices that are managed by the Configuration Manager client for Windows CE.
Client deployment failure for mobile devices that are managed by the Configuration Manager client for Windows CE	Displays detailed information about deployment failure for mobile devices that are managed by the Configuration Manager client for Windows CE.
Client deployment status details for mobile devices that are managed by the Configuration Manager client for Windows CE	Displays information about the status of mobile devices that are managed by the Configuration Manager client for Windows CE.
Client deployment success for mobile devices that are managed by the Configuration Manager client for Windows CE	Displays detailed information about deployment success for mobile devices that are managed by the Configuration Manager client for Windows CE.
Communication issues on mobile devices that are managed by the Configuration Manager client for Windows CE and that are not healthy	This report contains detailed information about communication issues on mobile devices that are managed by the Configuration Manager client for Windows CE.
Compliance status of default ActiveSync mailbox policy for the mobile devices that are managed by the Exchange Server connector	Displays a summary of the compliance status with the Default Exchange ActiveSync mailbox policy for the mobile devices managed by the Exchange Server connector.
Count of mobile devices by display configurations	This report displays the number of mobile devices by display settings.
Count of mobile devices by operating system	Displays the number of mobile devices by operating system.
Count of mobile devices by program memory	Displays the number of mobile devices by program memory.
Count of mobile devices by storage memory configurations	Count of mobile devices by storage memory configurations
Health information for mobile devices that are managed by the Configuration Manager client for Windows CE	Displays detailed health information for mobile devices that are managed by the Configuration Manager client for Windows CE.

REPORT NAME	DESCRIPTION
Health summary for mobile devices that are managed by the Configuration Manager client for Windows CE	Displays health summary information for mobile devices that are managed by the Configuration Manager client for Windows CE.
Inactive mobile devices that are managed by the Exchange Server connector	Displays the mobile devices managed by the Exchange Server connector that haven't connected to an Exchange Server in a specified number of days.
List of devices by Conditional Access State	Displays information about the current compliance and conditional access state of devices. You can use this report with conditional access policies. This report is available beginning in version 1602 of Configuration Manager.
List of devices by Health Attestation state	Displays a list of devices with attributes reported by Health Attestation Service
List of Devices enrolled per user in Microsoft Intune	Displays all devices a user has enrolled with Microsoft Intune.
List of devices in a specific device category	Displays information for all devices within a specific device category.
Local client issues on mobile devices that are managed by the Configuration Manager client for Windows CE and that are not healthy	This report contains detailed information about local client issues on mobile devices that are managed by the Configuration Manager client for Windows CE.
Mobile device client information	Displays information about the mobile devices that have the Configuration Manager client installed. You can use this report to verify which mobile devices can successfully communicate with a management point.
Mobile device compliance details for the Exchange Server connector	Displays the mobile device compliance details for a default Exchange ActiveSync mailbox policy that is configured by using the Exchange Server connector.
Mobile devices by operating system	Displays the mobile devices by operating system.
Mobile devices that are jailbroken or a rooted device	Displays the mobile devices that are jailbroken or a rooted device.
Mobile devices that are unmanaged because they enrolled but failed to assign to a site	Displays the mobile devices that completed enrollment with Configuration Manager, have a certificate, but failed to complete site assignment.
Mobile devices with a specific amount of free program memory	Displays all mobile devices with their specified amount of free program memory.
Mobile devices with a specific amount of free removable storage memory	Displays all mobile devices with the specified amount of free removable memory.
Mobile devices with certificate renewal issues	Displays the enrolled mobile devices that failed to renew their certificate. If you don't renew the certificate before the expiry period, the mobile devices become unmanaged.
Mobile devices with low free program memory (less than specified KB free)	Displays the mobile devices for which the program memory is lower than a specified size in KB.

REPORT NAME	DESCRIPTION
Mobile devices with low free removable storage memory (less than specified KB free)	Displays the mobile devices for which the removable storage memory is lower than a specified size in KB.
Number of devices enrolled per user in Microsoft Intune	Displays the users enabled for the Microsoft Intune subscription. It also shows the total number of devices enrolled for each user.
Pending retire and wipe request for mobile devices	Displays the wipe requests that are pending for mobile devices.
Recently enrolled and assigned mobile devices	Displays mobile devices that recently enrolled with Configuration Manager and successfully assigned to a site.
Recently wiped mobile devices	Displays the list of mobile devices that were recently successfully wiped.
Settings summary for mobile devices that are managed by the Exchange Server connector	Displays the number of mobile devices that apply the settings for each Default Exchange ActiveSync mailbox policy managed by the Exchange Server connector.
Windows RT Sideloading Keys Detailed Status	Displays detailed status information for a specified Windows RT sideloading key.
Windows RT Sideloading Keys Summary	Displays the status of Windows RT sideloading keys.

Driver management

The following 13 reports are listed under the **Driver Management** category.

REPORT NAME	DESCRIPTION
All drivers	Displays a list of all drivers.
All drivers for a specific platform	Displays all drivers for a specified platform.
All drivers in a specific boot image	Displays all drivers in a specified boot image.
All drivers in a specific category	Displays all drivers in a specified category.
All drivers in a specific package	Displays all drivers in a specified package.
Categories for a specific driver	Displays categories for a specified driver.
Computers that failed to install drivers for a specific collection	Displays computers that failed to install drivers for a specified collection.
Driver catalog matching report for a specific collection	Displays the driver catalog matching report for a specified collection.

REPORT NAME	DESCRIPTION
Driver catalog matching report for a specific computer	Displays the driver catalog matching report for a specified computer.
Driver catalog matching report for a specific device on a specific computer	Displays the driver catalog matching report for a specified device on a specified computer.
Driver catalog matching report for computers in a specific collection with a specific device	Displays driver catalog matching report for computers in a specified collection with a specified device.
Drivers that failed to install on a specific computer	Displays drivers that failed to install on a specified computer.
Supported platforms for a specific Driver	Displays supported platforms for a specified driver.

Endpoint Protection

The following six reports are listed under the **Endpoint Protection** category.

REPORT NAME	DESCRIPTION
Antimalware activity report	Displays an overview of antimalware activity.
Antimalware overall status and history	Displays the antimalware overall status and history.
Computer malware details	Displays details about a specified computer and the list of malware found on it.
Infected computers	Displays a list of computers with a specified threat detected.
Top users by threats	Displays the list of users with the most number of detected threats.
User threat list	Displays the list of threats found for a specified user account.

Hardware - CD-ROM

The following four reports are listed under the **Hardware - CD-ROM** category.

REPORT NAME	DESCRIPTION
CD-ROM information for a specific computer	Displays information about the CD-ROM drives on a specified computer.
Computers for a specific CD-ROM manufacturer	Displays a list of computers that contain a CD-ROM drive made by a manufacturer you specify.
Count CD-ROM drives per manufacturer	Displays the number of CD-ROM drives inventoried per manufacturer.
History - CD-ROM history for a specific computer	Displays the inventory history for CD-ROM drives on a specified computer.

Hardware - Disk

The following eight reports are listed under the **Hardware - Disk** category.

REPORT NAME	DESCRIPTION
Computers with a specific hard disk size	Displays a list of computers that have hard disks of a specified size.
Computers with low free disk space (less than specified % free)	Displays a list of computers in a specified collection that have less that the specified free disk space.
Computers with low free disk space (less that specified MB free)	Displays a list of computers and disks where the disks are low on space. The amount of free space to check for is specified in MB.
Count physical disk configurations	Displays the number of hard disks inventoried by disk capacity.
Disk information for a specific computer - Logical disks	Displays summary information about the logical disks on a specified computer.
Disk information for a specific computer - Partitions	Displays summary information about the disk partitions on a specified computer.
Disk information for a specific computer - Physical disks	Displays summary information about the physical disks on a specified computer.
History - Logical disk space history for a specific computer	Displays the inventory history for logical disk drives on a specified computer.

Hardware - General

The following five reports are listed under the **Hardware - General** category.

REPORT NAME	DESCRIPTION
Computer information for a specific computer	Displays summary information for a specified computer.
Computers in a specific workgroup or domain	Displays a list of computers in a specified Workgroup or domain.
Inventory classes assigned to a specific collection	Displays the inventory classes that are assigned to a specified collection.
Inventory classes enabled on a specific computer	Displays the inventory classes that are enabled on a specified computer.
Windows AutoPilot Device Information	Displays client device information that is needed for Windows AutoPilot registration.

Hardware - Memory

The following five reports are listed under the **Hardware - Memory** category.

REPORT NAME	DESCRIPTION
Computers where physical memory has changed	Displays a list of computers where the amount of RAM has changed since the last inventory cycle.
Computers with a specific amount of memory	Displays a list of computers that have a specified amount of RAM (Total Physical Memory rounded to the nearest MB).
Computers with low memory (less than or equal to specified MB)	Displays a list of computers that are low on memory. The amount of memory to check for is specified in MB.
Count memory configurations	Displays the number of computers inventoried by amount of RAM.
Memory information for a specific computer	Displays summary information about the memory on a specified computer.

Hardware - Modem

The following three reports are listed under the **Hardware - Modem** category.

REPORT NAME	DESCRIPTION
Computers for a specific modem manufacturer	Displays a list of computers that have a modem made by a specified manufacturer.
Count modems by manufacturer	Displays the number of modems inventoried for each modem manufacturer.
Modem information for a specific computer	Displays summary information about the modem on a specified computer.

Hardware - Network adapter

The following three reports are listed under the **Hardware - Network Adapter** category.

REPORT NAME	DESCRIPTION
Computers with a specific network adapter	Displays a list of computers that have a specified network adapter.
Count network adapters by type	Displays the number of inventoried network adapters cards of each type.
Network adapter information for a specific computer	Displays information about the network adapters installed on a specified computer.

Hardware - Processor

The following five reports are listed under the **Hardware - Processor** category.

REPORT NAME	DESCRIPTION
Computers for a specific processor speed	Displays a list of computers that have a processor of a specified speed.
Computers with fast processors (greater than or equal to a specified clock speed)	Displays a list of computers that have processors with a speed that is faster than the specified speed.
Computers with slow processors (less than or equal to a specified clock speed)	Displays a list of computers that have processors that run at or slower than a specified clock speed.
Count processor speeds	Displays the number of computers inventoried by processor speed.
Processor information for a specific computer	Displays information about the processors installed on a specified computer.

Hardware - SCSI

The following five reports are listed under the **Hardware - SCSI** category.

REPORT NAME	DESCRIPTION
Computers with a specific SCSI card type	Displays a list of computers that have a specified SCSI card installed.
Count SCSI card types	Displays the number of inventoried SCSI cards by card type.
SCSI card information for a specific computer	Displays information about the SCSI cards installed on a specified computer.

Hardware - Security

The following one report is listed under the **Hardware - Security** category.

REPORT NAME	DESCRIPTION
Details of firmware states on devices	Displays the details of the states of UEFI, SecureBoot, and TPM. **Note**: This report isn't in version 1810.

Hardware - Sound card

The following three reports are listed under the **Hardware - SCSI** category.

REPORT NAME	DESCRIPTION
Computers with a specific sound card	Displays a list of computers that have a specified sound card.
Count sound cards	Displays the number of computers inventoried by each sound card type.
Sound card information for a specific computer	Displays summary information about the sound cards on a specified computer.

Hardware - Video card

The following three reports are listed under the **Hardware - Video Card** category.

REPORT NAME	DESCRIPTION
Computers with a specific video card	Displays a list of computers that have a specified video card.
Count video cards by type	Displays a list of all of the video cards installed on computers. It also shows the number of each type of video card.
Video card information for a specific computer	Displays summary information about the video cards installed on a specified computer.

Migration

The following five reports are listed under the **Migration** category.

REPORT NAME	DESCRIPTION
Clients in exclusion list	Displays clients that are excluded from migration.
Dependency on a Configuration manager collection	Displays the objects that depend on a collection of the source hierarchy.
Migration job properties	This report shows the contents of the specified migration job.
Migration jobs	This report shows the list of migration jobs.
Objects that failed to migrate	Displays a list of objects that failed to migrate during the last attempt.

Network

The following six reports are listed under the **Network** category.

REPORT NAME	DESCRIPTION
Count IP addresses by subnet	Displays the number of IP addresses inventoried for each IP subnet.
IP - All subnets by subnet mask	Displays a list of IP subnets and subnet masks.
IP - Computers in a specific subnet	Displays a list of computers and IP information for a specified IP subnet.
IP - Information for a specific computer	Displays summary information about IP on a specified computer.
IP - Information for a specific IP address	Displays summary information about a specified IP address.
MAC - Computers for a specific MAC address	Displays the computer name and IP address of computers that have the specified MAC address.

Operating system

The following 10 reports are listed under the **Operating System** category.

REPORT NAME	DESCRIPTION
Computer operating system version history	Displays the inventory history for the operating system on a specified computer.
Computers with a specific operating system	Displays computers with a specified operating system.
Computers with a specific operating system and service pack	Displays computers with a specified operating system and service pack.
Count operating system versions	Displays the number of computers inventoried by operating system.
Count operating systems and service packs	Displays the number of computers inventoried by operating system and service pack combinations.
Services - Computers running a specific service	Displays a list of computers running a specified service.
Services - Computers running Remote Access Server	Displays a list of computers running Remote Access Server.
Services - Services information for a specific computer	Displays summary information about the services on a specified computer.
Windows 10 Servicing details for a specific collection	Displays general information about Windows 10 servicing for a specific collection.
Windows Server computers	Displays a list of computers that run Windows Server operating systems.

Power management

The following 18 reports are listed under the **Power Management** category.

REPORT NAME	DESCRIPTION
Power Management - Computer activity	Displays a graph showing monitor, computer, and user activity for a specified collection over a specified time period.
Power Management - Computer activity by computer	Displays a graph showing monitor, computer, and user activity for a specified computer on a specified date.
Power Management - Computer activity details	Displays a list of the sleep and wake capabilities of computers in the specified collection for a specified date and time.
Power Management - Computer details	Displays detailed information about the power capabilities, power settings, and power plans applied to a specified computer.
Power Management - Computer not reporting details	Displays a list of computers not reporting any power activity for a specified date and time.

REPORT NAME	DESCRIPTION
Power Management - Computers excluded	Displays a list of computers excluded from the power plan.
Power Management - Computers with multiple power plans	Displays a list of computers that have multiple, conflicting power settings applied.
Power Management - Energy consumption	Displays the total monthly energy consumption (in kWh) for a specified collection over a specified time period.
Power Management - Energy consumption by day	Displays the total energy consumption (in kWh) for a specified collection in the last 31 days.
Power Management - Energy cost	Displays the total monthly energy consumption cost for a specified collection over a specified time period.
Power Management - Energy cost by day	Displays the total energy consumption cost for a specified collection over the past 31 days.
Power Management - Environmental impact	Displays a graph showing carbon dioxide (CO2) emissions generated by a specified collection over a specified time period.
Power Management - Environmental impact by day	Displays a graph showing CO2 emissions generated by a specified collection over the past 31 days.
Power Management - Insomnia computer details	Displays detailed information about computers that didn't sleep or hibernate within a specified time period.
Power Management - Insomnia report	Displays a list of common causes that prevented computers from sleeping or hibernating. It also shows the number of computers affected by each cause over a specified time period.
Power Management - Power capabilities	Displays the power management capabilities of computers in the specified collection.
Power Management - Power settings	Displays an aggregated list of power settings used by computers in a specified collection.
Power Management - Power settings details	Used to display further information about computers that were specified in the **Power Management - Power settings** report.

Replication traffic

The following 10 reports are listed under the **Replication Traffic** category.

REPORT NAME	DESCRIPTION
Global Data Replication Traffic Per Link (line chart)	Displays total global data replication traffic on a specified link for a specified number of days.
Global Data Replication Traffic Per Link (pie chart)	Displays total global data replication traffic on a specified link for a specified number of days.

REPORT NAME	DESCRIPTION
Hierarchy Replication Traffic By Link	Displays total replication traffic for each link in the hierarchy for a specified number of days.
Hierarchy Top Ten Replication Groups Traffic Per Link (pie chart)	Displays the replication traffic for the top 10 replication groups across the entire hierarchy identified by link.
Link Replication Traffic	Displays total replication traffic for all data for a specified number of days.
Replication group traffic per link	Displays the replication group network traffic over a specified database replication link for a specified number of days.
Site Data Replication Traffic Per Link (line chart)	Displays total site data replication traffic on a specified link for a specified number of days.
Site Data Replication Traffic Per Link (pie chart)	Displays total site data replication traffic on a specified link for a specified number of days.
Total Hierarchy Replication Traffic (line chart)	Displays hierarchy aggregate global and site data replication for each direction of every link for a specified number of days.
Total Hierarchy Replication Traffic (pie chart)	Displays hierarchy aggregate global and site data replication for each direction of every link for a specified number of days.

Site - Client information

The following 19 reports are listed under the **Site - Client Information** category.

REPORT NAME	DESCRIPTION
Client assignment detailed status report	Displays detailed information about client assignment status.
Client assignment failure details	Displays detailed information about client assignment failures.
Client assignment status details	Displays overview information about client assignment status.
Client assignment success details	Displays detailed information about successfully assigned clients.
Client deployment failure report	Displays detailed information for clients that have failed to deploy.
Client deployment status details	Displays summary information for the status of client installations.
Client deployment success report	Displays detailed information for clients that have successfully deployed.
Clients incapable of HTTPS communication	Displays detailed information about each client that runs the HTTPS Communication Readiness Tool, and reports to be incapable of communicating over HTTPS.

REPORT NAME	DESCRIPTION
Computers assigned but not installed for a particular site	Displays a list of computers assigned to a specified site, but aren't reporting to that site.
Computers with a specific Configuration Manager client version	Displays a list of computers running a specified version of the Configuration Manager client software.
Count of clients and protocol used for communication	Displays a summary of the communication methods used by clients (HTTP or HTTPS).
Count of clients assigned and installed for each site	Displays the number of computers assigned and installed for each site. Clients with a network location associated to multiple sites are only counted as installed if they're reporting to that site.
Count of clients capable of HTTPS communication	Displays detailed information about each client that runs the HTTPS Communication Readiness Tool, and reports to be either capable or incapable of communicating over HTTPS.
Count of clients for each site	Displays the number of Configuration Manager clients installed by site code.
Count of Configuration Manager clients by client versions	Displays the number of computers discovered by Configuration Manager client version.
Problem details reported to the fallback status point for a specified collection	Displays detailed information for issues reported by clients in a specified collection. These clients must have an assigned fallback status point.
Problem details reported to the fallback status point for a specified site	Displays detailed information about issues reported by clients in a specified site. These clients must have an assigned fallback status point.
Summary of problems reported to the fallback status point	Displays information about all the issues reported by clients. These clients must have an assigned fallback status point.
Summary of problems reported to the fallback status point for a specific collection	Displays summary information for issues reported by clients in a specified collection. These clients must have an assigned fallback status point.

Site - Discovery and inventory information

The following 10 reports are listed under the **Site - Discovery and Inventory Information** category.

REPORT NAME	DESCRIPTION
Clients that have not reported recently (in a specified number of days)	Displays a list of clients that haven't reported discovery data, hardware inventory, or software inventory in a specified number of days.
Computers discovered by a specific site	Displays a list of all computers that the specified site discovered. It also shows the date of the most recent discovery.

REPORT NAME	DESCRIPTION
Computers discovered recently by discovery method	Displays a list of computers that the site discovered within the specified number of days. It also lists the agents that discovered them. If multiple agents discovered a computer, it may appear more than once in the list.
Computers not discovered recently (in a specified number of days)	Displays a list of computers that the site hasn't recently discovered. It also shows the number of days since the site discovered the computer.
Computers not inventoried recently (in a specified number of days)	Displays a list of computers that the site hasn't recently inventoried. It also shows the last times the client inventoried the computer.
Computers that might share the same Configuration Manager unique identifier	Displays a list of computers that have changed their names. A change in name is a possible symptom that a computer shares a Configuration Manager Unique Identifier with another computer.
Computers with duplicate MAC addresses	Displays computers that share MAC address.
Count computers in resource domains or workgroups	Displays the number of computers in each resource domain or workgroup.
Discovery information for a specific computer	Displays a list of the agents and sites that discovered a specified computer.
Inventory dates for a specific computer	Displays the date and time inventory was last run on a specified computer.

Site - General

The following three reports are listed under the **Site - General** category.

REPORT NAME	DESCRIPTION
Computers in a specific site	Displays a list of client computers in a specified site.
Site status for the hierarchy	Displays the list of sites in the hierarchy with site version and site status information.
Status of Configuration Manager update within hierarchy	Displays information about Configuration Manager site updates for the hierarchy.

Site - Server information

The following one report is listed under the **Site - Server Information** category.

REPORT NAME	DESCRIPTION
Site system roles and site system servers for a specific site	Displays a list of site system server and their site system roles for a specified site.

Software - Companies and products

The following 15 reports are listed under the **Software - Companies and Products** category.

REPORT NAME	DESCRIPTION
All inventoried products for a specific software company	Displays a list of the inventoried software products and versions from a specified software company.
All software companies	Displays a list of all companies manufacturing inventoried software.
All Windows apps	Displays a summary of installed Windows apps. It searches using the following criteria: application name, architecture, or publisher.
Computers with a specific product	Displays a list of the computers that a specified product is inventoried on, and the versions of that product.
Computers with a specific product name and version	Displays a list of the computers that a specified version of a product is inventoried on.
Computers with specific software registered in Add Remove Programs	Displays a summary of all computers with specified software registered in Add Remove Programs or Programs and Features.
Count all inventoried products and versions	Displays a list of the inventoried software products and versions, and the number of computers each is installed on.
Count inventoried products and versions for a specific product	Displays a list of the inventoried versions of a specified product, and the number of computers each is installed on.
Count of all instances of software registered with Add or Remove Programs	Displays a summary of all instances of software installed and registered with Add or Remove Programs or Programs and Features on computers within the specified collection.
Count of instances of specific software registered with Add or Remove Programs	Displays a count of instances for specified software packages installed and registered in Add or Remove Programs or Programs and Features.
Default Browser counts	Shows the count of clients with a specific web browser as the Windows default. Use the following reference for common BrowserProgIDs: - AppXq0fevzme2pys62n3e0fbqa7peapykr8v: Microsoft Edge - IE.HTTP: Microsoft Internet Explorer - ChromeHTML: Google Chrome - OperaStable: Opera Software - FirefoxURL-308046B0AF4A39CB: Mozilla Firefox - Unknown: the client OS doesn't support the query, the query hasn't run, or a user hasn't logged on
Installations of specified Windows apps	This report lists all computers with a specified Windows app.
Products on a specific computer	Displays a summary of the inventoried software products and their manufacturers on a specified computer.

REPORT NAME	DESCRIPTION
Software registered in Add Remove Programs on a specific computer	Displays a summary of the software installed on a specified computer that is registered in Add Remove Programs or Programs and Features.
Windows apps installed to the specified user	Displays all Windows apps installed to the specified user

Software - Files

The following five reports are listed under the **Software - Files** category.

REPORT NAME	DESCRIPTION
All inventoried files for a specific product	Display a summary of the files inventoried that are associated with a specified software product.
All inventoried files on a specific computer	Display a summary of all the files inventoried on a specified computer.
Compare software inventory on two computers	Displays the differences between the software inventories reported for two specified computers.
Computers with a specific file	Displays a list of computers that have collected software inventory for a specified file name. If a computer contains multiple copies of the file, it might appear more than once in the list.
Count computers with a specific file name	Displays the number of computers that have collected software inventory for a specified file.

Software distribution - Application monitoring

The following 10 reports are listed under the **Software Distribution - Application Monitoring** category.

REPORT NAME	DESCRIPTION
All application deployments (advanced)	Displays detailed summary information for all application deployments.
All application deployments (basic)	Displays summary information for all application deployments.
Application compliance	Displays compliance information for the specified application within the specified collection.
Application deployments per asset	Displays applications deployed to a specified device or user.
Application infrastructure errors	Displays application infrastructure errors. These errors include internal infrastructure issues, or errors resulting from invalid requirement rules.
Application Usage Detailed Status	Displays usage details for installed applications.
Application Usage Summary Status	Displays a usage summary for installed applications.

REPORT NAME	DESCRIPTION
iOS apps with failed deployments (app already installed)	Displays compliance information for the selected iOS app. You deployed this app as an 'App package for iOS from App Store', which you also associated with a mobile application management policy. This report is used to display users and devices for which the app failed to install because it had already been manually installed by the user.
Task sequence deployments containing application	Displays task sequence deployments that install a specified application.
User Requests for Android Application	Displays users that requested to install an Android application.

Software distribution - Collections

The following three reports are listed under the **Software Distribution - Collections** category.

REPORT NAME	DESCRIPTION
All collections	Displays all the collections in the hierarchy.
All resources in a specific collection	Displays all the resources in a specified collection.
Maintenance windows available to a specified client	Displays all maintenance windows that are applicable to the specified client.

Software distribution - Content

The following 16 reports are listed under the **Software Distribution - Content** category.

REPORT NAME	DESCRIPTION
All active content distributions	Displays all distributions points on which content is currently being installed or removed.
All content	Displays all applications and packages at a site.
All content on a specific distribution point	Displays all content currently installed on a specified distribution point.
All distribution points	Displays information about the distribution points for each site.
All status messages for a specific package on a specific distribution point	Displays all status messages for a specified package on a specified distribution point.
Application content distribution status	Displays information about the distribution status for application content.
Applications targeted to distribution point group	Displays information about application content that was deployed to a specified distribution point group.

REPORT NAME	DESCRIPTION
Applications that are out of synchronization on a specified distribution point group	Displays the applications for which associated content files haven't been updated with the latest version on a specified distribution point group.
Distribution point group	Displays information about a specified distribution point group.
Distribution point usage summary	Displays the distribution point usage summary for each distribution point.
Distribution status of specified package	Displays the distribution status for specified package content on each distribution point.
Packages targeted to distribution point group	Displays information about packages that target a specified distribution point group.
Packages that are out of synchronization on a specified distribution point group	Displays packages for which associated content files haven't been updated with the latest version on a specified distribution point group.
Peer cache source content rejection	Displays the number of peer cache source rejections per boundary group.
Peer cache source content rejection by condition	Displays the peer cache sources that rejected to serve content based on a condition.
Peer cache source content rejection details	Displays the name of the content that was rejected by a peer source.

Software distribution - Package and program deployment

The following five reports are listed under the **Software Distribution - Package and Program Deployment** category.

REPORT NAME	DESCRIPTION
All deployments for a specified package and program	Displays information about all deployments of a specified package and program.
All package and program deployments	Displays all of the package and program deployments at this site.
All package and program deployments to a specified collection	Displays all of the package and program deployments to a specified collection.
All package and program deployments to a specified computer	Displays all of the package and program deployments that apply to a specified computer.
All package and program deployments to a specified user	Displays all of the package and program deployments to a specified user.

Software distribution - Package and program deployment status

The following five reports are listed under the **Software Distribution - Package and Program Deployment Status** category.

REPORT NAME	DESCRIPTION
All system resource package and program deployments with status	Displays all package and program deployments for the site with a summary status of each deployment.
All system resources for a specified package and program deployment in a specified state	Displays a list of resources that are in a specified state for a specified package and program deployment.
Chart - Hourly package and program deployment completion status	Displays the percentage of computers that successfully installed the package. The list organizes for every hour since an administrator creates the package and program deployment. It can be used to track the average time for a package and program deployment.
Package and program deployment status for a specified client and deployment	Displays the status messages reported for a specified computer and package and program deployment.
Status of a specified package and program deployment	Displays the status summary for a specified package and program deployment.

Software metering

The following 13 reports are listed under the **Software Metering** category.

REPORT NAME	DESCRIPTION
All software metering rules applied to this site	Displays a list of all software metering rules at the site.
Computers that have a metered program installed but haven't run the program since a specified date	Displays all computers with the specified metered application, but no user has run the program since the specified date.
Computers that have run a specific metered software program	Displays a list of computers that have run programs matching the specified software metering rule within the specified month and year.
Concurrent usage for all metered software programs	Displays the maximum number of users who concurrently ran each metered software program during the specified month and year.
Concurrent usage trend analysis of a specific metered software program	Displays the maximum number of users who concurrently ran the specified metered software program during each month for the past year.
Install base for all metered software programs	Displays the number of computers that have metered software programs installed as reported by software inventory. This report requires that the computer collects software inventory.
Software metering summarization progress	Displays the time at which the most recently summarized metering data was processed on the site server. The software metering reports only reflect metering data processed before these dates.

REPORT NAME	DESCRIPTION
Time of day usage summary for a specific metered software program	Displays the average number of usages of a particular program for the past 90 days, broken down by hour and day.
Total usage for all metered software programs	Displays the number of users who ran programs within the specified month and year, and that match each software metering rule. These rules are for locally installed software, or using Terminal Services.
Total usage for all metered software programs on Windows Terminal Servers	Displays the number of users who ran programs matching each software metering rule using Terminal Services within the specified month and year.
Total usage trend analysis for a specific metered software program	Displays the number of users who ran programs during each month for the past year, and that match the specified software metering rule. These rules are for locally installed software, or using Terminal Services.
Total usage trend analysis for a specific metered software program on Windows Terminal Servers	Displays the number of users who ran programs during each month for the past year, and that match the specified software metering rule. These rules are for using Terminal Services.
Users that have run a specific metered software program	Displays a list of users who have run programs within the specified month and year, and that match the specified software metering rule.

Software updates - A Compliance

The following eight reports are listed under the **Software Updates - A Compliance** category.

REPORT NAME	DESCRIPTION
Compliance 1 - Overall compliance	Displays the overall compliance data for a software update group.
Compliance 2 - Specific software update	Displays the compliance data for a specified software update.
Compliance 3 - Update group (per update)	Displays the compliance data for software updates defined in a software update group.
Compliance 4 - Updates by vendor month year	Displays the compliance data for software updates released by a vendor during a specified month and year.
Compliance 5 - Specific computer	This report returns the software update compliance data for a specified computer. To limit the amount of information returned, you can specify the vendor and software update classification.
Compliance 6 - Specific software update states (secondary)	Displays the count and percentage of computers in each compliance state for the specified software update.
Compliance 7 - Computers in a specific compliance state for an update group (secondary)	Displays all computers in a collection that have a specified overall compliance state against a software update group.

REPORT NAME	DESCRIPTION
Compliance 8 - Computers in a specific compliance state for an update (secondary)	Displays all computers in a collection that have a specified compliance state for a software update.
Compliance 9 - Overall health and compliance	Displays the overall health and compliance data for a software update group. (starting in version 1806)

Software updates - B Deployment management

The following eight reports are listed under the **Software Updates - B Deployment Management** category.

REPORT NAME	DESCRIPTION
Management 1 - Deployments of an update group	Displays all deployments that include all of the software updates defined in a specified software update group.
Management 2 - Updates required but not deployed	Displays all vendor-specific software updates that clients detect as required, but an administrator hasn't deployed to a specified collection.
Management 3 - Updates in a deployment	Displays the software updates that are contained in a specified deployment.
Management 4 - Deployments that target a collection	Displays all software update deployments that target a specified collection.
Management 5 - Deployments that target a computer	Displays all software update deployments that are deployed to a specified computer.
Management 6 - Deployments that contain a specific update	Displays all deployments that include a specified software update and the associated target collection for the deployment.
Management 7 - Updates in a deployment missing content	Displays the software updates in a specified deployment that don't have all of the associated content retrieved. This state prevents clients from installing the update, which prevents the deployment from achieving 100% compliance.
Management 8 - Computers missing content (secondary)	Displays all computers requiring the specified software update, but the associated content isn't yet distributed to a distribution point.

Software updates - C Deployment states

The following six reports are listed under the **Software Updates - C Deployment States** category.

REPORT NAME	DESCRIPTION
States 1 - Enforcement states for a deployment	Displays the enforcement states for a specified software update deployment, which is typically the second phase of a deployment assessment.

REPORT NAME	DESCRIPTION
States 2 - Evaluation states for a deployment	Displays the evaluation state for a specified software update deployment, which is typically the first phase of a deployment assessment.
States 3 - States for a deployment and computer	Displays the states for all software updates in the specified deployment for a specified computer.
States 4 - Computers in a specific state for a deployment (secondary)	Displays all computers in a specified state for a software update deployment.
States 5 - States for an update in a deployment (secondary)	Displays a summary of states for a specified software update targeted by a specified deployment.
States 6 - Computers in a specific enforcement state for an update (secondary)	Displays all computers in a specified enforcement state for a specified software update.

Software updates - D Scan

The following four reports are listed under the **Software Updates - D Scan** category.

REPORT NAME	DESCRIPTION
Scan 1 - Last scan states by collection	Specify a collection to display the count of computers in each compliance scan state. The clients return the state during the last compliance scan.
Scan 2 - Last scan states by site	Specify a site to display the count of computers in each compliance scan state. The clients return the state during the last compliance scan.
Scan 3 - Clients of a collection reporting a specific state (secondary)	Displays all computers for a specified collection and a specified compliance scan state during their last compliance scan.
Scan 4 - Clients of a site reporting a specific state (secondary)	Specify a site to display all computers with a specified compliance scan state. The clients return the state during their last compliance scan.

Software updates - E Troubleshooting

The following four reports are listed under the **Software Updates - E Troubleshooting** category.

REPORT NAME	DESCRIPTION
Troubleshooting 1 - Scan errors	Displays scan errors at the site and a count of computers that are experiencing each error.
Troubleshooting 2 - Deployment errors	Displays the deployment errors at the site and a count of computers that are experiencing each error.
Troubleshooting 3 - Computers failing with a specific scan error (secondary)	Displays a list of the computers that failed a scan because of a specified error.

REPORT NAME	DESCRIPTION
Troubleshooting 4 - Computers failing with a specific deployment error (secondary)	Displays a list of the computers on which the deployment of update is failing because of a specified error.

State migration

The following three reports are listed under the **State Migration** category.

REPORT NAME	DESCRIPTION
State migration information for a specific source computer	Displays state migration information for a specified computer.
State migration information for a specific state migration point	Displays state migration information for a specified state migration point.
State migration points for a specific site	Displays the state migration points for a specified site.

Status messages

The following 12 reports are listed under the **Status Messages** category.

REPORT NAME	DESCRIPTION
All messages for a specific message ID	Displays a list of status messages that have a specified message ID.
Clients reporting errors in the last 12 hours for a specific site	Displays a list of computers and components reporting errors in the last 12 hours, and the number of errors reported.
Component messages for the last 12 hours	Displays a list of component messages for the last 12 hours for a specified site code, computer, and component.
Component messages for the last hour	Displays a list of the status messages created in the last hour by a specified component on a specified computer at a specified site.
Count component messages for the last hour for a specific site	Displays the number of status messages by component and severity reported in the last hour at a specified site.
Count errors in the last 12 hours	Displays the number of server component error status messages in the last 12 hours.
Fatal errors (by component)	Displays a list of computers reporting fatal errors by component.
Fatal errors (by computer name)	Displays a list of computers reporting fatal errors by computer name.
Last 1000 messages for a specific computer (Errors and Warnings)	Displays a summary of the last 1000 error and warning component status messages for a specified computer.

REPORT NAME	DESCRIPTION
Last 1000 messages for a specific computer (Errors Warnings and Information)	Displays a summary of the last 1000 error, warning, and informational component status messages for a specified computer.
Last 1000 messages for a specific computer (Errors)	Displays a summary of the last 1000 error server component status messages for a specified computer.
Last 1000 messages for a specific server component	Displays a summary of the most recent 1000 status messages for a specified server component.

Status messages - Audit

The following three reports are listed under the **Status Messages - Audit** category.

REPORT NAME	DESCRIPTION
All audit messages for a specific user	Displays a summary of all audit status messages for a specified user. Audit messages describe actions taken in the Configuration Manager console that add, modify, or delete objects in Configuration Manager.
Remote Control - All computers remote controlled by a specific user	Displays a summary of status messages indicating remote control of client computers by a specified user.
Remote Control - All remote control information	Displays a summary of status messages related to the remote control of client computers.

Task sequence - Deployment status

The following 11 reports are listed under the **Task Sequence - Deployment Status** category.

REPORT NAME	DESCRIPTION
All system resources for a task sequence deployment in a specific state	Displays a list of the destination computers for the specified task sequence deployment in a specified deployment state.
All system resources for a task sequence deployment that is in a specific state and that is available to unknown computers	Displays a list of the destination computers for the specified task sequence deployment that is in the specified deployment state.
Count of system resources that have task sequence deployments assigned but not yet run	Displays the number of computers that have accepted task sequences, but haven't run the task sequence.
History of a task sequence deployment on a computer	Displays the status of each step of the specified task sequence deployment on the specified destination computer. If no record is returned, the task sequence hasn't started on the computer.
List of computers that exceeded a specific length of time to run a task sequence deployment	Displays the list of destination computers that exceeded the specified length of time to run a task sequence.
Run time for a specific task sequence deployment on a specific destination computer	Displays the total time that it took to successfully complete a specified task sequence on a specified computer.

REPORT NAME	DESCRIPTION
Run time for each step of a task sequence deployment on a specific destination computer	Displays the time that it took to complete each step of the specified task sequence deployment on the specified destination computer.
Status of a specific task sequence deployment for a specific computer	Displays the status summary of a specified task sequence deployment on a specified computer.
Status of a task sequence deployment on an unknown destination computer	Displays the status of the specified task sequence deployment on the specified unknown destination computer.
Status summary of a specific task sequence deployment	Displays a status summary of all resources that have been targeted by a deployment.
Status summary of a specific task sequence deployment available to unknown computers	Displays the status summary of all resources targeted by the specified deployment that is available to a collection containing unknown computers.

Task sequence - Deployments

The following 11 reports are listed under the **Task Sequence - Deployments** category.

REPORT NAME	DESCRIPTION
All system resources currently in a specific group or phase of a specific task sequence deployment	Displays a list of computers that are currently running in a specified group or phase of a specified task sequence deployment.
All system resources where a task sequence deployment failed within a specific group or phase	Displays a list of computers that failed within a specified group/phase of the specified task sequence deployment.
All task sequence deployments	Displays details of all task sequence deployments initiated from the current site.
All task sequence deployments available to unknown computers	Displays details of all the task sequence deployments initiated from the site, and deployed to collections that contain unknown computers.
Count of failures in each phase or group of a specific task sequence	Displays the number of failures in each phase or group of the specified task sequence.
Count of failures in each phase or group of a specific task sequence deployment	Displays the number of failures in each phase or group of the specified task sequence deployment.
Deployment status of all task sequence deployments	Displays the overall progress of all task sequence deployments.
Progress of a running task sequence	Displays the progress of the specified task sequence.
Progress of a running task sequence deployment	Displays the summary information for the specified task sequence deployment.
Progress of all deployments for a specific task sequence	Displays the progress of all deployments for the specified task sequence.

REPORT NAME	DESCRIPTION
Summary report for a task sequence deployment	Displays the summary information for the specified task sequence deployment.

Task sequence - Progress

The following five reports are listed under the **Task Sequence - Progress** category.

REPORT NAME	DESCRIPTION
Chart - Weekly progress of a task sequence	Displays the weekly progress of a task sequence, starting from the deployment date.
Progress of a task sequence	Displays the progress of the specified task sequence.
Progress of all task sequences	Displays a summary of the progress of all task sequences.
Progress of task sequences for operating system deployments	Displays the progress of all task sequences that deploy operating systems.
Status of all unknown computers	Displays a list of computers that were unknown at the time they ran a task sequence deployment, and whether they're now known computers.

Task sequences - References

The following one report is listed under the **Task Sequences - References** category.

REPORT NAME	DESCRIPTION
Content referenced by a specific task sequence	Displays content that is referenced by a specified task sequence.

User - Device affinity

The following two reports are listed under the **User - Device Affinity** category.

REPORT NAME	DESCRIPTION
Pending user device affinity associations by collection	This report shows all pending user device affinity assignments based on usage data, for members of a collection.
User device affinity associations per collection	Displays all user device associations for the specified collection, and groups the results by collection type (for example, user or device).

User data and profiles health

The following four reports are listed under the **User Data and Profiles Health** category.

REPORT NAME	DESCRIPTION
Folder Redirection Health Report - Details	Displays the health state details of folder redirection for each of the redirected folders for a given user.
Roaming User Profiles Health Report - Details	Displays the health state details of the roaming user profile for a specified user.
User Data and Profiles Health Report - Details	Displays the error or warning details of folder redirection or roaming user profiles. This report is the details target from the summary report.
User Data and Profiles Health Report - Summary	Displays the summary of health states for folder redirection and roaming user profiles.

Users

The following three reports are listed under the **Users** category.

REPORT NAME	DESCRIPTION
Computers for a specific user name	Displays a list of the computers that were used by a specified user.
Count users by domain	Displays the number of users in each domain.
Users in a specific domain	Displays a list of users and their computers in a specified domain.

Virtual applications

The following seven reports are listed under the **Virtual Applications** category.

REPORT NAME	DESCRIPTION
App-V Virtual Environment Results	Displays information about a specified virtual environment that is in a specified state for a specified collection.
App-V Virtual Environment Results For Asset	Displays information about a specified virtual environment for a specified asset. It also shows any deployment types for the specified virtual environment.
App-V Virtual Environment Status	Displays compliance information for a specified virtual environment for a specified collection.
Computers with a specific virtual application	Displays a summary of computers that have the specified App-V application shortcut as created using the Application Virtualization Management Sequencer.
Computers with a specific virtual application package	Displays a summary of computers that have the specified App-V application package.
Count of all instances of virtual application packages	Display a count of detected App-V application packages.

REPORT NAME	DESCRIPTION
Count of all instances of virtual applications	Display a count of detected App-V applications.

Volume purchase programs - Apple

The following report is listed under the **Volume Purchase Programs - Apple** category.

REPORT NAME	DESCRIPTION
Apple Volume Purchase Program apps for iOS with license counts	Displays all iPhone, iPad, and iPod Touch applications licensed through Apple's Volume Purchase Program. This report also includes the total licenses purchased, and licenses consumed per application.

Vulnerability assessment

The following one report is listed under the **Vulnerability Assessment** category.

REPORT NAME	DESCRIPTION
Vulnerability Assessment Overall Report	Identifies security, administrative, and compliance vulnerabilities for a specific computer

Wake On LAN

The following seven reports are listed under the **Wake On LAN** category.

REPORT NAME	DESCRIPTION
All computers targeted for Wake On LAN activity	Specify the type of deployment to display a list of computers targeted for Wake on LAN activity.
All objects pending wake-up activity	Displays objects that are scheduled for wakeup.
All sites that are enabled for Wake On LAN	Displays a list of all sites in the hierarchy that are enabled for Wake On LAN.
Errors received while sending wake-up packets for a defined period	Displays errors received while sending wake-up packets to computers for a defined period.
History of Wake On LAN activity	Displays a history of the wakeup activity that has occurred since a certain period.
Wake-Up Proxy Deployment State Details	Displays information about the deployment status of Wake-Up Proxy for each device in a specified collection.
Wake-Up Proxy Deployment State Summary	Displays a summary of the deployment status of wake-up proxy for a specified collection.

Configure reporting in Configuration Manager

8/23/2019 • 13 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Before you can create, modify, and run reports in the Configuration Manager console, there are several configuration tasks to complete. Use this article to help you configure reporting in your Configuration Manager hierarchy.

Before you install and configure SQL Server Reporting Services in your hierarchy, review the following Configuration Manager reporting articles:

- Introduction to reporting in Configuration Manager
- Planning for reporting in Configuration Manager

SQL Server Reporting Services

SQL Server Reporting Services is a server-based reporting platform that provides comprehensive reporting functionality for different kinds of data sources. The reporting services point in Configuration Manager communicates with SQL Server Reporting Services to:

- Copy Configuration Manager reports to a specified report folder
- Configure Reporting Services settings
- Configure Reporting Services security settings

When you run a report, the Reporting Services component connects to the Configuration Manager site database to retrieve data.

Before you can install the reporting services point in a Configuration Manager site, install and configure SQL Server Reporting Services on the target site system. For more information, see Install SQL Server Reporting Services.

Use the following procedure to verify that SQL Server Reporting Services is installed and running correctly.

1. Go to the **Start** menu on the site system, and open **Reporting Services Configuration Manager**. You may find it in the **Configuration Tools** section of the **Microsoft SQL Server** group.
2. In the **Reporting Services Configuration Connection** window, enter the name of the server that hosts SQL Server Reporting Services. Select the instance of SQL Server on which you installed SQL Reporting Services. Then select **Connect** to open Reporting Services Configuration Manager.
3. On the **Report Server Status** page, verify that **Report Service Status** is **Started**. If it's not in this state, select **Start**.
4. On the **Web Service URL** page, select the URL in **Report Service Web Service URLs**. This action tests the connection to the report folder. The browser might prompt you for credentials. Verify that the webpage opens successfully.
5. On the **Database** page, verify that the **Report Server Mode** is set to **Native**.
6. On the **Report Manager URL** page, select the URL in **Report Manager Site Identification**. This action tests the connection to the virtual directory for Report Manager. The browser might prompt you for credentials. Verify that the webpage opens successfully.

> **NOTE**
> Reporting in Configuration Manager doesn't require Reporting Services Report Manager. You only need it if you want to run reports in the browser or manage reports by using Report Manager.

7. Select **Exit** to close Reporting Services Configuration Manager.

Configure reporting to use Report Builder 3.0

1. On the computer running the Configuration Manager console, open the Windows Registry Editor.
2. Browse to **HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Microsoft/ConfigMgr10/AdminUI/Reporting**.
3. Open the **ReportBuilderApplicationManifestName** key to edit the value data.
4. Change **ReportBuilder_2_0_0_0.application** to **ReportBuilder_3_0_0_0.application**, and then select **OK**.
5. Close the Windows Registry Editor.

Install a reporting services point

To manage reports at the site, install the reporting services point. The reporting services point:

- Copies report folders and reports to SQL Server Reporting Services
- Applies the security policy for the reports and folders
- Sets configuration settings in Reporting Services

Requirements and limitations

Before you can view or manage reports in the Configuration Manager console, you need a reporting services point. Configure this site system role on a server with Microsoft SQL Server Reporting Services. For more information, see Prerequisites for reporting.

- When you select a site to install the reporting services point, users who will access the reports must be in the same security scope as the site where you install the role.
- After you install a reporting services point on a site system, don't change the URL for the report server.

  For example, you create the reporting services point. You then modify the URL for the report server in Reporting Services Configuration Manager. The Configuration Manager console continues to use the old URL. You can't run, edit, or create reports from the console.

  If you need to change the report server URL, first remove the existing reporting services point. Change the URL, and then reinstall the reporting services point.
- When you install a reporting services point, specify a Reporting services point account. For users from a different domain to run a report, create a two-way trust between domains. Otherwise the report fails to run.

Install the reporting services point on a site system

For more information about configuring site systems, see Install site system roles.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and then select the **Servers and Site System Roles** node.

2. Add the reporting services point to a new or existing site system server:

   - *New site system*: On the **Home** tab of the ribbon, in the **Create** group, select **Create Site System Server**. The **Create Site System Server Wizard** opens.
   - *Existing site system*: Select the target server. On the **Home** tab of the ribbon, in the **Server** group, select **Add Site System Role**. The **Add Site System Roles Wizard** opens.

3. On the **General** page, specify the general settings for the site system server. When you add the reporting services point to an existing server, verify the values that you previously configured.

4. On the **System Role Selection** page, select **Reporting services point** in the list of available roles, and then select **Next**.

5. On the **Reporting services point** page, configure the following settings:

   - **Site database server name**: Specify the name of the server that hosts the Configuration Manager site database. The wizard typically retrieves the fully qualified domain name (FQDN) for the server. To specify a database instance, use the format *<server name><instance name>*. For example, `sqlserver\named1`.
   - **Database name**: Specify the Configuration Manager site database name. Select **Verify** to confirm that the wizard has access to the site database.

     > **IMPORTANT**
     > The user account you use to create the reporting services point must have **Read** access to the site database. If the connection test fails, a red warning icon appears. Contextual hover text on the icon has the details of the failure. Correct the failure, and then select **Test** again.

   - **Folder name**: Specify the folder name to create and use for Configuration Manager reports in Reporting Services.
   - **Reporting Services server instance**: Select the instance of SQL Server for Reporting Services. If this page doesn't list any instances, verify that SQL Server Reporting Services is installed, configured, and started.

     > **IMPORTANT**
     > Configuration Manager makes a connection in the context of the current user to WMI on the selected site system. It uses this connection to retrieve the instance of SQL Server for Reporting Services. The current user must have **Read** access to WMI on the site system, or the wizard can't get the Reporting Services instances.

   - **Reporting services point account**: Select **Set**, and then select an account to use. SQL Server Reporting Services on the reporting services point uses this account to connect to the Configuration Manager site database. This connection is to retrieve the data for a report. Select **Existing account** to specify a Windows user account that you previously configured as a Configuration Manager account. Select **New account** to specify a Windows user account that's not currently configured for use. Configuration Manager automatically grants the specified user access to the site database.

     The account that runs Reporting Services must belong to the domain local security group **Windows Authorization Access Group**. It also needs the **Read tokenGroupsGlobalAndUniversal** permission set to **Allow**. Users in a different domain than the reporting services point account need a two-way trust between the domains to successfully run reports.

The specified Windows user account and password are encrypted and stored in the Reporting Services database. Reporting Services retrieves the data for reports from the site database by using this account and password.

> **IMPORTANT**
> The account that you specify must have the **Log on locally** permission on the server that hosts the Reporting Services database.

6. Complete the wizard.

After the wizard completes, Configuration Manager creates the report folders in Reporting Services. It then copies its reports to the specified report folders.

> **TIP**
> To list only site systems that host the reporting services point site role, right-click **Servers and Site System Roles**, and select **Reporting services point**.

Languages for reports

When Configuration Manager creates report folders and copies reports to the report server, it determines the appropriate language for the objects.

- Create report folders, copy reports
  - Create objects using locale of the site server OS
  - If the specific language pack isn't available, default to English (ENU)
- View reports in a web browser
  - Folder and report names: the same locale as the site server
  - Report contents: dynamic based on the browser locale
- View reports in the Configuration Manager console
  - Folder and report names: dynamic based on the locale of the console
  - Report contents: dynamic based on the locale of the console

When you install a reporting services point on a site without language packs, the reports are installed in English. If you install a language pack after you install the reporting services point, you must uninstall and reinstall the reporting services point for the reports to be available in the appropriate language pack language.

For more information, see Language packs.

File installation and report folder security rights

Configuration Manager does the following actions to install the reporting services point and to configure Reporting Services:

> **IMPORTANT**
> The site does these actions in the context of the account that's configured for the SMS_Executive service. Typically, this account is the site server local System account.

- Install the reporting services point site role.

- Create the data source in Reporting Services with the stored credentials that you specified in the wizard. This account is the Windows user account and password that Reporting Services uses to connect to the site database when you run reports.
- Create the Configuration Manager root folder in Reporting Services.
- Add the **ConfigMgr Report Users** and **ConfigMgr Report Administrators** security roles in Reporting Services.
- Create subfolders, and then deploy Configuration Manager reports from `%ProgramFiles%\SMS_SRSRP` on the site server to Reporting Services.
- Add the **ConfigMgr Report Users** role in Reporting Services to the root folders for all user accounts in Configuration Manager that have **Site Read** rights.
- Add the **ConfigMgr Report Administrators** role in Reporting Services to the root folders for all user accounts in Configuration Manager that have **Site Modify** rights.
- Retrieve the mapping between report folders and Configuration Manager secured object types. Configuration Manager maintains this map in the site database.
- Configure the following rights for administrative users in Configuration Manager to specific report folders in Reporting Services:
  - Add users and assign the **ConfigMgr Report Users** role to the associated report folder for administrative users who have **Run Report** permissions for the Configuration Manager object.
  - Add users and assign the **ConfigMgr Report Administrators** role to the associated report folder for administrative users who have **Modify Report** permissions for the Configuration Manager object.

Configuration Manager connects to Reporting Services and sets the permissions for users on the Configuration Manager and Reporting Services root folders and specific report folders. After the initial installation of the reporting services point, Configuration Manager connects to Reporting Services every 10 minutes to verify that the user rights configured on the report folders are the associated rights that are set for Configuration Manager users. When users are added or user rights are modified on the report folder by using Reporting Services Report Manager, Configuration Manager overwrites those changes by using the role-based assignments stored in the site database. Configuration Manager also removes users that don't have Reporting rights in Configuration Manager.

Reporting Services security roles

When Configuration Manager installs the reporting services point, it adds the following security roles in Reporting Services:

- **ConfigMgr Report Users**: Users assigned with this security role can only run Configuration Manager reports.
- **ConfigMgr Report Administrators**: Users assigned with this security role can do all tasks related to reporting in Configuration Manager.

Verify installation

Verify the installation of the reporting services point by looking at specific status messages and log file entries. Use the following procedure to verify that the reporting services point installation was successful.

> **NOTE**
>
> If you see reports in the **Reports** subfolder of the **Reporting** node in the **Monitoring** workspace in the Configuration Manager console, you can skip this procedure.

Verify installation by status message

1. In the Configuration Manager console, go to the **Monitoring** workspace, expand **System Status**, and select the **Component Status** node.
2. Select the **SMS_SRS_REPORTING_POINT** component.
3. On the **Home** tab of the ribbon, in the **Component** group, select **Show Messages**, and then choose **All**.
4. Specify a date and time for a period before you installed the reporting services point, and then select **OK**.
5. Verify status message ID **1015**. This status message indicates that the reporting services point was successfully installed.

Verify installation by log file

Open the **Srsrp.log** file, located in the **Logs** directory of the Configuration Manager installation path. Look for the string `Installation was successful`.

Step through this log file starting from the time that the reporting services point was successfully installed. Verify that the report folders were created, the reports were deployed, and the security policy on each folder was confirmed. After the last line of security policy confirmations, look for the string `Successfully checked that the SRS web service is healthy on server`.

Configure a certificate to author reports

There are many options for you to author reports in SQL Server Reporting Services. When you create or edit reports in the Configuration Manager console, Configuration Manager opens Report Builder to use as the authoring environment. Regardless of how you author your Configuration Manager reports, you need a self-signed certificate for server authentication to the site database server.

> **NOTE**
>
> For more information about authoring reports with SQL Server Reporting Services, see Report Builder authoring environment.

Configuration Manager automatically installs the certificate on the site server and any SMS Provider roles. You can create or edit reports from the Configuration Manager console when you run it from one of these servers.

When you create or modify reports from a Configuration Manager console on a different computer, export the certificate from the site server. The specific certificate's friendly name is the FQDN of the site server in the **Trusted People** certificate store for the local computer. Add this certificate to the **Trusted People** certificate store on the computer that runs the Configuration Manager console.

Modify reporting services point settings

After you install this role, you can modify the site database connection and authentication settings in the reporting services point properties.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and then select the **Servers and Site System Roles** node.

> **TIP**
> To list only site systems that host the reporting services point, right-click the **Servers and Site System Roles** node, and select **Reporting services point**.

2. Select the site system that hosts the reporting services point. Then select the **Reporting service point** site system roles in the details pane.
3. On the **Site Role** tab of the ribbon, in the **Properties** group, select **Properties**.
4. You can modify the following settings in the **Reporting Services Point Properties**:
   - **Site database server name**
   - **Database name**
   - **User account**
5. Select **OK** to save the changes and close the properties.

For more information about these settings, see the descriptions in the section to Install the reporting services point on a site system.

Upgrade SQL Server

To upgrade SQL Server and SQL Server Reporting Services, first remove the reporting services point from the site. After you upgrade SQL Server, then reinstall the reporting services point in Configuration Manager.

If you don't follow this process, you'll see errors when you run or edit reports from the Configuration Manager console. You can continue to run and edit reports successfully from a web browser.

Configure report options

You can select the default reporting services point that you use to manage reports. The site can have more than one reporting services point, but it only uses the default server to manage reports. Use the following procedure to configure report options for your site.

1. In the Configuration Manager console, go to the **Monitoring** workspace, expand **Reporting**, and then select the **Reports** node.
2. On the **Home** tab of the ribbon, in the **Settings** group, select **Report Options**.
3. Select the default report server in the list, and then select **OK**.

If it doesn't show any servers, verify that you installed and configured a reporting services point in the site. For more information, see Verify installation.

Make sure your computer runs a version of SQL Server Report Builder that matches the version of SQL Server that you use for your report server. Otherwise you'll see an error, the default report server won't save, and you can't create or edit reports.

Next steps

Operations and maintenance for reporting

Operations and maintenance for reporting in System Center Configuration Manager

9/5/2019 • 18 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

After the infrastructure is in place for reporting in System Center Configuration Manager, there are a number of operations that you typically perform to manage reports and report subscriptions.

Manage Configuration Manager reports

Configuration Manager provides over 400 predefined reports that help you gather, organize, and present information about users, hardware and software inventory, software updates, applications, site status, and other Configuration Manager operations in your organization. You can use the predefined reports as they are, or you can modify a report to meet your requirements. You can also create custom model-based and SQL-based reports to meet your requirements. Use the following sections to help you manage Configuration Manager reports.

Run a Configuration Manager report

Reports in Configuration Manager are stored in SQL Server Reporting Services, and the data rendered in the report is retrieved from the Configuration Manager site database. You can access reports in the Configuration Manager console or by using Report Manager, which you access in a web browser. You can open reports on any computer that has access to the computer that is running SQL Server Reporting Services, and you must have sufficient rights to view the reports. When you run a report, the report title, description, and category are displayed in the language of the local operating system.

> **NOTE**
> In some non-English languages, characters may not appear correctly in reports. In this case, reports can be viewed using the web-based Report Manager or through the Remote Administrator Console.

> **WARNING**
> To run reports, you must have **Read** rights for the **Site** permission and the **Run Report** permission that is configured for specific objects.

> **IMPORTANT**
> There must be a two-way trust established for users from a different domain than that of the Reporting Servicies Point Account to successfully run reports.

> **NOTE**
> Report Manager is a web-based report access and management tool that you use to administer a single report server instance on a remote location over an HTTP connection. You can use Report Manager for operational tasks, for example, to view reports, modify report properties, and manage associated report subscriptions. This topic provides the steps to view a report and modify report properties in Report Manager, but for more information about the other options that Report Manager provides, see Report Manager in SQL Server 2008 Books Online.

Use the following procedures to run a Configuration Manager report.

To run a report in the Configuration Manager console

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, expand **Reporting**, and then click **Reports** to list the available reports.

   > **IMPORTANT**
   > In this version of Configuration Manager, the **All content** reports only display packages, not applications.

   > **TIP**
   > If no reports are listed, verify that the reporting services point is installed and configured. For more information, see Configuring reporting.

3. Select the report that you want to run, and then on the **Home** tab, in the **Report Group** section, click **Run** to open the report.
4. When there are required parameters, specify the parameters, and then click **View Report**.

To run a report in a web browser

1. In your web browser, enter the Report Manager URL, for example, **http://Server1/Reports**. You can determine the Report Manager URL on the **Report Manager URL** page in Reporting Services Configuration Manager.
2. In Report Manager, click the report folder for Configuration Manager, for example, **ConfigMgr_CAS**.

   > **TIP**
   > If no reports are listed, verify that the reporting services point is installed and configured. For more information, see Configuring reporting.

3. Click the report category for the report that you want to run, and then click the link for the report. The report opens in Report Manager.
4. When there are required parameters, specify the parameters, and then click **View Report**.

Modify the properties for a Configuration Manager report

In the Configuration Manager console, you can view the properties for a report, such as the report name and description, but to change the properties, use Report Manager. Use the following procedure to modify the properties for a Configuration Manager report.

To modify report properties in Report Manager

1. In your web browser, enter the Report Manager URL, for example, **http://Server1/Reports**. You can determine the Report Manager URL on the **Report Manager URL** page in Reporting Services Configuration Manager.
2. In Report Manager, click the report folder for Configuration Manager, for example, **ConfigMgr_CAS**.

   > **TIP**
   > If no reports are listed, verify that the Reporting Services point is installed and configured. For more information, see Configuring reporting

3. Click the report category for the report for which you want to modify properties, and then click the link for the report. The report opens in Report Manager.
4. Click the **Properties** tab. You can modify the report name and description.
5. When you are finished, click **Apply**. The report properties are saved on the report server, and the Configuration Manager console retrieves the updated report properties for the report.

Edit a Configuration Manager report

When an existing Configuration Manager report does not retrieve the information that you have to have or does not provide the layout or design that you want, you can edit the report in Report Builder.

> **NOTE**
> You can also choose to clone an existing report by opening it for editing, and clicking **Save As** to save it as a new report.

> **IMPORTANT**
> The user account must have **Site Modify** permission and **Modify Report** permissions on the specific objects associated with the report that you want to modify.

> **IMPORTANT**
> When Configuration Manager is upgraded to a newer version, new reports overwrite the predefined reports. If you modify a predefined report, you must back up the report before you install the new version, and then restore the report in Reporting Services. If you are making significant changes to a predefined report, consider creating a new report instead. New reports that you create before you upgrade a site are not overwritten.

Use the following procedure to edit the properties for a Configuration Manager report.

To edit report properties

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, expand **Reporting**, and then click **Reports** to list the available reports.
3. Select the report that you want to modify, and then on the **Home** tab, in the **Report Group** section, click **Edit**. Enter your user account and password if you are prompted, and then click **OK**. If Report Builder is not installed on the computer, you are prompted to install it. Click **Run** to install Report Builder, which is required to modify and create reports.
4. In Report Builder, modify the appropriate report settings, and then click **Save** to save the report to the report server.

Create a model-based report

A model-based report lets you interactively select the items you want to include in your report. For more information about creating custom report models, see Creating custom report models for System Center Configuration Manager in SQL Server Reporting Services.

> **IMPORTANT**
> The user account must have **Site Modify** permission to create a new report. The user can only create a report in folders for which the user has **Modify Report** permissions.

Use the following procedure to create a model-based Configuration Manager report.

To create a model-based report

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, expand **Reporting** and click **Reports**.
3. On the **Home** tab, in the **Create** section, click **Create Report** to open the **Create Report Wizard**.
4. On the **Information** page, configure the following settings:
   - **Type**: Select **Model-based Report** to create a report in Report Builder by using a Reporting Services model.
   - **Name**: Specify a name for the report.
   - **Description**: Specify a description for the report.
   - **Server**: Displays the name of the report server on which you are creating this report.
   - **Path**: Click **Browse** to specify a folder in which you want to store the report.

     Click **Next**.
5. On the **Model Selection** page, select an available model in the list that you use to create this report. When you select the report model, the **Preview** section displays the SQL Server views and entities that are made available by the selected report model.
6. On the **Summary** page, review the settings. Click **Previous** to change the settings or click **Next** to create the report in Configuration Manager.
7. On the **Confirmation** page, click **Close** to exit the wizard, and then open Report Builder to configure the report settings. Enter your user account and password if you are prompted, and then click **OK**. If Report Builder is not installed on the computer, you are prompted to install it. Click **Run** to install Report Builder, which is required to modify and create reports.
8. In Microsoft Report Builder, create the report layout, select data in the available SQL Server views, add parameters to the report, and so on. For more information about using Report Builder to create a new report, see the Report Builder Help.
9. Click **Run** to run your report. Verify that the report provides the information that you expect. Click **Design** to return to the Design view to modify the report, if needed.
10. Click **Save** to save the report to the report server. You can run and modify the new report in the **Reports** node in the **Monitoring** workspace.

Create a SQL-based report

A SQL-based report lets you retrieve data that is based on a report SQL statement.

> **IMPORTANT**
> When you create an SQL statement for a custom report, do not directly reference SQL Server tables. Instead, reference reporting SQL Server views (view names that start with v_) from the site database. You can also reference public stored procedures (stored procedure names that start with sp_) from the site database.

> **IMPORTANT**
> The user account must have **Site Modify** permission to create a new report. The user can only create a report in folders for which the user has **Modify Report** permissions.

Use the following procedure to create a SQL-based Configuration Manager report.

To create a SQL-based report

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, expand **Reporting**, and then click **Reports**.
3. On the **Home** tab, in the **Create** section, click **Create Report** to open the **Create Report Wizard**.
4. On the **Information** page, configure the following settings:
   - **Type**: Select **SQL-based Report** to create a report in Report Builder by using a SQL statement.
   - **Name**: Specify a name for the report.
   - **Description**: Specify a description for the report.
   - **Server**: Displays the name of the report server on which you are creating this report.
   - **Path**: Click **Browse** to specify a folder in which you want to store the report.

     Click **Next**.
5. On the **Summary** page, review the settings. Click **Previous** to change the settings or click **Next** to create the report in Configuration Manager.
6. On the **Confirmation** page, click **Close** to exit the wizard and open Report Builder to configure the report settings. Enter your user account and password if you are prompted, and then click **OK**. If Report Builder is not installed on the computer, you are prompted to install it. Click **Run** to install Report Builder, which is required to modify and create reports.
7. In Microsoft Report Builder, provide the SQL statement for the report or build the SQL statement by using columns in available SQL Server views, add parameters to the report, and so on.
8. Click **Run** to run your report. Verify that the report provides the information that you expect. Click **Design** to return to the Design view to modify the report, if needed.
9. Click **Save** to save the report to the report server. You can run the new report in the **Reports** node in the **Monitoring** workspace.

Manage report subscriptions

Report subscriptions in SQL Server Reporting Services let you configure the automatic delivery of specified reports by email or to a file share at scheduled intervals. Use the **Create Subscription Wizard** in System Center 2012 Configuration Manager to configure report subscriptions.

Create a report subscription to deliver a report to a file share

When you create a report subscription to deliver a report to a file share, the report is copied in the specified format to the file share that you specify. You can subscribe to and request delivery for only one report at a time.

Unlike reports that are hosted and managed by a report server, reports that are delivered to a shared folder are static files. Interactive features that are defined for the report do not work for reports that are stored as files on the file system. Interaction features are represented as static elements. If the report includes charts, the default presentation is used. If the report links through to another report, the link is rendered as static text. If you want to retain interactive features in a delivered report, use email delivery instead. For more information about email delivery, see the Create a report subscription to deliver a report by email section later in this topic.

When you create a subscription that uses file share delivery, you must specify an existing folder as the destination folder. The report server does not create folders on the file system. The folder that you specify must be accessible over a network connection. When you specify the destination folder in a subscription, use a UNC path and do not

include trailing backslashes in the folder path. For example, a valid UNC path for the destination folder is: \\<servername>\reportfiles\operations\2011.

Reports can be rendered in a variety of file formats, such as MHTML or Excel. To save the report in a specific file format, select that rendering format when creating your subscription. For example, choosing Excel saves the report as a Microsoft Excel file. Although you can select any supported rendering format, some formats work better than others when rendering to a file.

Use the following procedure to create a report subscription to deliver a report to a file share.

To create a report subscription to deliver a report to a file share

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, expand **Reporting** and click **Reports** to list the available reports. You can select a report folder to list only the reports that are associated with the folder.
3. Select the report that you want to add to the subscription, and then on the **Home** tab, in the **Report Group** section, click **Create Subscription** to open the **Create Subscription Wizard**.
4. On the **Subscription Delivery** page, configure the following settings:
   - Report delivered by: Select **Windows File Share** to deliver the report to a file share.
   - **File Name**: Specify the file name for the report. By default, the report file does not include a file name extension. Select **Add file extension when created** to automatically add a file name extension to this report based on the render format.
   - **Path**: Specify a UNC path to an existing folder where you want to deliver this report (for example, \\<server name>\<server share>\<report folder>).

     > **NOTE**
     > The user name specified later on this page must have access to this server share and have Write permissions on the destination folder.

   - **Render Format**: Select one of the following formats for the report file:
     - **XML file with report data**: Saves the report in Extensible Markup Language format.
     - **CSV (comma delimited)**: Saves the report in comma-separated-value format.
     - **TIFF file**: Saves the report in Tagged Image File Format.
     - **Acrobat (PDF) file**: Saves the report in Acrobat Portable Document Format.
     - **HTML 4.0**: Saves the report as a webpage viewable only in browsers that support HTML 4.0. Internet Explorer 5 and later versions support HTML 4.0.

       > **NOTE**
       > If you have images in your report, the HTML 4.0 format does not include them in the file.

     - **MHTML (web archive)**: Saves the report in MIME HTML format (mhtml), which is viewable in many web browsers.
     - **RPL Renderer**: Saves the report in Report Page Layout (RPL) format.
     - **Excel**: Saves the report as a Microsoft Excel spreadsheet.

- **Word**: Saves the report as a Microsoft Word document.

- **User Name**: Specify a Windows user account with permissions to access the destination server share and folder. The user account must have access to this server share and have Write permission on the destination folder.
- **Password**: Specify the password for the Windows user account. In **Confirm Password**, re-enter the password.
- Select one of the following options to configure the behavior when a file of the same name exists in the destination folder:
  - **Overwrite an existing file with a newer version**: Specifies that when the report file already exists, the new version overwrites it.
  - **Do not overwrite an existing file**: Specifies that when the report file already exists, there is no action.
  - **Increment file names as newer versions are added**: Specifies that when the report file already exists, a number is added to the new report to the file name to distinguish it from other versions.
- **Description**: Specifies the description for the report subscription.

  Click **Next**.

5. On the **Subscription Schedule** page, select one of the following delivery schedule options for the report subscription:
   - **Use shared schedule**: A shared schedule is a previously defined schedule that can be used by other report subscriptions. Select this check box, and then select a shared schedule in the list if any have been specified.
   - **Create new schedule**: Configure the schedule on which this report runs, including the interval, start time and date, and the end date for this subscription.
6. On the **Subscription Parameters** page, specify the parameters for this report that are used when it is run unattended. When there are no parameters for the report, this page is not displayed.
7. On the **Summary** page, review the report subscription settings. Click **Previous** to change the settings or click **Next** to create the report subscription.
8. On the **Completion** page, click **Close** to exit the wizard. Verify that the report subscription was created successfully. You can view and modify report subscriptions in the **Subscriptions** node under **Reporting** in the **Monitoring** workspace.

Create a report subscription to deliver a report by email

When you create a report subscription to deliver a report by email, an email is sent to the recipients that you configure, and the report is included as an attachment. The report server does not validate email addresses or obtain email addresses from an email server. You must know in advance which email addresses you want to use. By default, you can email reports to any valid email account within or outside of your organization. You can select one or both of the following email delivery options:

- Send a notification and a hyperlink to the generated report.
- Send an embedded or attached report. The rendering format and browser determine whether the report is embedded or attached. If your browser supports HTML 4.0 and MHTML, and you select the MHTML (web archive) rendering format, the report is embedded as part of the message. All other rendering formats (CSV, PDF, Word, and so on) deliver reports as attachments. Reporting Services does not check the size of

the attachment or message before sending the report. If the attachment or message exceeds the maximum limit allowed by your mail server, the report is not delivered.

> **IMPORTANT**
> You must configure the email settings in Reporting Services for the **Email** delivery option to be available. For more information about configuring the email settings in Reporting Services, see Configuring a Report Server for Email Delivery in the SQL Server Books Online.

Use the following procedure to create a report subscription to deliver a report by using email.

To create a report subscription to deliver a report by email

- In the Configuration Manager console, click **Monitoring**.
- In the **Monitoring** workspace, expand **Reporting** and click **Reports** to list the available reports. You can select a report folder to list the only the reports that are associated with the folder.
- Select the report that you want to add to the subscription, and then on the **Home** tab, in the **Report Group** section, click **Create Subscription** to open the **Create Subscription Wizard**.
- On the **Subscription Delivery** page, configure the following settings:
  - **Report delivered by**: Select **E-mail** to deliver the report as an attachment in an email message.
  - **To**: Specify a valid email address to send this report to.

    > **NOTE**
    > You can enter multiple email recipients by separating each email address with a semicolon.

  - **Cc**: Optionally, specify an email address to copy this report to.
  - **Bcc**: Optionally, specify an email address to send a blind copy of this report to.
  - **Reply To**: Specify the reply address to use if the recipient replies to the email message.
  - **Subject**: Specify a subject line for the subscription email message.
  - **Priority**: Select the priority flag for this email message. Select **Low**, **Normal**, or **High**. The priority setting is used by Microsoft Exchange to set a flag indicating the importance of the email message.
  - **Comment**: Specify text to be added to the body of the subscription email message.
  - **Description**: Specify the description for this report subscription.
  - **Include Link**: Includes a URL to the subscribed report in the body of the email message.
  - **Include Report**: Specify that the report is attached to the e-mail message. The format in which the report will be attached is specified in the **Render Format** list.
  - **Render Format**: Select one of the following formats for the attached report:
    - **XML file with report data**: Saves the report in Extensible Markup Language format.
    - **CSV (comma delimited)**: Saves the report in comma-separated-value format.
    - **TIFF file**: Saves the report in Tagged Image File Format.
    - **Acrobat (PDF) file**: Saves the report in Acrobat Portable Document Format.
    - **MHTML (web archive)**: Saves the report in MIME HTML format (mhtml), which is viewable

in many web browsers.

- **Excel**: Saves the report as a Microsoft Excel spreadsheet.
- **Word**: Saves the report as a Microsoft Word document.

- On the **Subscription Schedule** page, select one of the following delivery schedule options for the report subscription:
  - **Use shared schedule**: A shared schedule is a previously defined schedule that can be used by other report subscriptions. Select this check box, and then select a shared schedule in the list if any have been specified.
  - **Create new schedule**: Configure the schedule on which this report will run, including the interval, start time and date, and the end date for this subscription.
- On the **Subscription Parameters** page, specify the parameters for this report that are used when it is run unattended. When there are no parameters for the report, this page is not displayed.
- On the **Summary** page, review the report subscription settings. Click **Previous** to change the settings or click **Next** to create the report subscription.
- On the **Completion** page, click **Close** to exit the wizard. Verify that the report subscription was created successfully. You can view and modify report subscriptions in the **Subscriptions** node under **Reporting** in the **Monitoring** workspace.

Creating custom report models for System Center Configuration Manager in SQL Server Reporting Services

2/12/2019 • 17 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Sample report models are included in System Center Configuration Manager, but you can also define report models to meet your own business requirements, and then deploy the report model to Configuration Manager to use when you create new model-based reports. The following table provides the steps to create and deploy a basic report model.

> **NOTE**
> For the steps to create a more advanced report model, see the Steps for Creating an Advanced Report Model in SQL Server Reporting Services section in this topic.

STEP	DESCRIPTION	MORE INFORMATION
Verify that SQL Server Business Intelligence Development Studio is installed	Report models are designed and built by using SQL Server Business Intelligence Development Studio. Verify that SQL Server Business Intelligence Development Studio is installed on the computer on which you are creating the custom report model.	For more information about SQL Server Business Intelligence Development Studio, see the SQL Server 2008 documentation.
Create a report model project	A report model project contains the definition of the data source (a .ds file), the definition of a data source view (a .dsv file), and the report model (an .smdl file).	For more information, see the To create the report model project section in this topic.
Define a data source for a report model	After creating a report model project, you have to define one data source from which you extract business data. Typically, this is the Configuration Manager site database.	For more information, see the To define the data source for the report model section in this topic.

STEP	DESCRIPTION	MORE INFORMATION
Define a data source view for a report model	After defining the data sources that you use in your report model project, the next step is to define a data source view for the project. A data source view is a logical data model based on one or more data sources. Data source views encapsulate access to the physical objects, such as tables and views, contained in underlying data sources. SQL Server Reporting Services generates the report model from the data source view. Data source views facilitate the model design process by providing you with a useful representation of the data that you specified. Without changing the underlying data source, you can rename tables and fields, and add aggregate fields and derived tables in a data source view. For an efficient model, add only those tables to the data source view that you intend to use.	For more information, see the To define the data source view for the report model section in this topic.
Create a report model	A report model is a layer on top of a database that identifies business entities, fields, and roles. When published, by using these models, Report Builder users can develop reports without having to be familiar with database structures or understand and write queries. Models are composed of sets of related report items that are grouped together under a friendly name, with predefined relationships between these business items and with predefined calculations. Models are defined by using an XML language called Semantic Model Definition Language (SMDL). The file name extension for report model files is .smdl.	For more information, see the To create the report model section in this topic.
Publish a report model	To build a report by using the model that you just created, you must publish it to a report server. The data source and data source view are included in the model when it is published.	For more information, see the To publish the report model for use in SQL Server Reporting Services section in this topic.
Deploy the report model to Configuration Manager	Before you can use a custom report model in the **Create Report Wizard** to create a model-based report, you must deploy the report model to Configuration Manager.	For more information, see the To deploy the custom report model to Configuration Manager section in this topic.

Steps for creating a basic report model in SQL Server Reporting Services

You can use the following procedures to create a basic report model that users in your site can use to build

particular model-based reports based on data in a single view of the Configuration Manager database. You create a report model that presents information about the client computers in your site to the report author. This information is taken from the **v_R_System** view in the Configuration Manager database.

On the computer where you perform these procedures, ensure that you have installed SQL Server Business Intelligence Development Studio and that the computer has network connectivity to the reporting services point server. For detailed information about SQL Server Business Intelligence Development Studio, see the SQL Server 2008 documentation.

To create the report model project

1. On the desktop, click **Start**, click **Microsoft SQL Server 2008**, and then click **SQL Server Business Intelligence Development Studio**.
2. After **SQL Server Business Intelligence Development Studio** opens in Microsoft Visual Studio, click **File**, click **New**, and then click **Project**.
3. In the **New Project** dialog box, select **Report Model Project** in the **Templates** list.
4. In the **Name** box, specify a name for this report model. For this example, type **Simple_Model**.
5. To create the report model project, click **OK**.
6. The **Simple_Model** solution is displayed in **Solution Explorer**.

> **NOTE**
> If you cannot see the **Solution Explorer** pane, click **View**, and then click **Solution Explorer**.

To define the data source for the report model

1. In the **Solution Explorer** pane of **SQL Server Business Intelligence Development Studio**, right-click **Data Sources** to select **Add New Data Source**.
2. On the **Welcome to the Data Source Wizard** page, click **Next**.
3. On the **Select how to define the connection** page, verify that **Create a data source based on an existing or new connection** is selected, and then click **New**.
4. In the **Connection Manager** dialog box, specify the following connection properties for the data source:
   - **Server name**: Type the name of your Configuration Manager site database server, or select it in the list. If you are working with a named instance instead of the default instance, type *<database server>\<instance name>*.
   - Select **Use Windows Authentication**.
   - In **Select or enter a database name** list, select the name of your Configuration Manager site database.
5. To verify the database connection, click **Test Connection**.
6. If the connection succeeds, click **OK** to close the **Connection Manager** dialog box. If the connection does not succeed, verify that the information you entered is correct, and then click **Test Connection** again.
7. On the **Select how to define the connection** page, verify that **Create a data source based on an existing or new connection** is selected, verify that the data source you have just specified is selected in **Data connections**, and then click **Next**.
8. In **Data source name**, specify a name for the data source, and then click **Finish**. For this example, type **Simple_Model**.

9. The data source **Simple_Model.ds** is now displayed in **Solution Explorer** under the **Data Sources** node.

> **NOTE**
> To edit the properties of an existing data source, double-click the data source in the **Data Sources** folder of the **Solution Explorer** pane to display the data source properties in Data Source Designer.

To define the data source view for the report model

1. In **Solution Explorer**, right-click **Data Source Views** to select **Add New Data Source View**.
2. On the **Welcome to the Data Source View Wizard** page, click **Next**. The **Select a Data Source** page is displayed.
3. In the **Relational data sources** window, verify that the **Simple_Model** data source is selected, and then click **Next**.
4. On the **Select Tables and Views** page, select the following view in the **Available objects** list to be used in the report model: **v_R_System (dbo)**.

> **TIP**
> To help locate views in the **Available objects** list, click the **Name** heading at the top of the list to sort the objects in alphabetical order.

5. After selecting the view, click **>** to transfer the object to the **Included objects** list.
6. If the **Name Matching** page is displayed, accept the default selections, and click **Next**.
7. When you have selected the objects that you require, click **Next**, and then specify a name for the data source view. For this example, type **Simple_Model**.
8. Click **Finish**. The **Simple_Model.dsv** data source view is displayed in the **Data Source Views** folder of **Solution Explorer**.

To create the report model

1. In **Solution Explorer**, right-click **Report Models** to select **Add New Report Model**.
2. On the **Welcome to the Report Model Wizard** page, click **Next**.
3. On the **Select Data Source Views** page, select the data source view in the **Available data source views** list, and then click **Next**. For this example, select **Simple_Model.dsv**.
4. On the **Select report model generation rules** page, accept the default values, and then click **Next**.
5. On the **Collect Model Statistics** page, verify that **Update model statistics before generating** is selected, and then click **Next**.
6. On the **Completing the Wizard** page, specify a name for the report model. For this example, verify that **Simple_Model** is displayed.
7. To complete the wizard and create the report model, click **Run**.
8. To exit the wizard, click **Finish**. The report model is shown in the Design window.

To publish the report model for use in SQL Server Reporting Services

1. In **Solution Explorer**, right-click the report model to select **Deploy**. For this example, the report model is **Simple_Model.smdl**.

2. Examine the deployment status at the lower left corner of the **SQL Server Business Intelligence Development Studio** window. When the deployment has finished, **Deploy Succeeded** is displayed. If the deployment fails, the reason for the failure is displayed in the **Output** window. The new report model is now available on your SQL Server Reporting Services website.
3. Click **File**, click **Save All**, and then close **SQL Server Business Intelligence Development Studio**.

To deploy the custom report model to Configuration Manager

1. Locate the folder in which you created the report model project. For example, %*USERPROFILE*%\Documents\Visual Studio 2008\Projects\<*Project Name*>.
2. Copy the following files from the report model project folder to a temporary folder on your computer:
   - <*Model Name*> **.dsv**
   - <*Model Name*> **.smdl**
3. Open the preceding files by using a text editor, such as Notepad.
4. In the file <*Model Name*>**.dsv**, locate the first line of the file, which reads as follows:

   <DataSourceView xmlns="http://schemas.microsoft.com/analysisservices/2003/engine">

   Edit this line to read as follows:

   <DataSourceView xmlns="http://schemas.microsoft.com/analysisservices/2003/engine" xmlns:xsi="RelationalDataSourceView">
5. Copy the entire contents of the file to the Windows Clipboard.
6. Close the file <*Model Name*>**.dsv**.
7. In the file <*Model Name*>**.smdl**, locate the last three lines of the file, which appear as follows:

   ```
   </Entity>
   ```

   ```
   </Entities>
   ```

   ```
   </SemanticModel>
   ```
8. Paste the contents of the file <*Model Name*>**.dsv** directly before the last line of the file (**<SemanticModel>**).
9. Save and close the file <*Model Name*>**.smdl**.
10. Copy the file <*Model Name*>**.smdl** to the folder *%programfiles%*\Microsoft Configuration Manager \AdminConsole\XmlStorage\Other on the Configuration Manager site server.

> **IMPORTANT**
> After copying the report model file to the Configuration Manager site server, you must exit and restart the Configuration Manager console before you can use the report model in the **Create Report Wizard**.

Steps for Creating an Advanced Report Model in SQL Server Reporting Services

You can use the following procedures to create an advanced report model that users in your site can use to build particular model-based reports based on data in multiple views of the Configuration Manager database. You create a report model that presents information about the client computers and the operating system installed on

these computers to the report author. This information is taken from the following views in the Configuration Manager database:

- **V_R_System**: Contains information about discovered computers and the Configuration Manager client.
- **V_GS_OPERATING_SYSTEM**: Contains information about the operating system installed on the client computer.

  Selected items from the preceding views are consolidated into one list, given friendly names, and then presented to the report author in Report Builder for inclusion in particular reports.

  On the computer where you perform these procedures, ensure that you have installed SQL Server Business Intelligence Development Studio and that the computer has network connectivity to the reporting services point server. For detailed information about SQL Server Business Intelligence Development Studio, see the SQL Server documentation.

To create the report model project

1. On the desktop, click **Start**, click **Microsoft SQL Server 2008**, and then click **SQL Server Business Intelligence Development Studio**.
2. After **SQL Server Business Intelligence Development Studio** opens in Microsoft Visual Studio, click **File**, click **New**, and then click **Project**.
3. In the **New Project** dialog box, select **Report Model Project** in the **Templates** list.
4. In the **Name** box, specify a name for this report model. For this example, type **Advanced_Model**.
5. To create the report model project, click **OK**.
6. The **Advanced_Model** solution is displayed in **Solution Explorer**.

> **NOTE**
> If you cannot see the **Solution Explorer** pane, click **View**, and then click **Solution Explorer**.

To define the data source for the report model

1. In the **Solution Explorer** pane of **SQL Server Business Intelligence Development Studio**, right-click **Data Sources** to select **Add New Data Source**.
2. On the **Welcome to the Data Source Wizard** page, click **Next**.
3. On the **Select how to define the connection** page, verify that **Create a data source based on an existing or new connection** is selected, and then click **New**.
4. In the **Connection Manager** dialog box, specify the following connection properties for the data source:
   - **Server name**: Type the name of your Configuration Manager site database server, or select it in the list. If you are working with a named instance instead of the default instance, type *<database server>\<instance name>*.
   - Select **Use Windows Authentication**.
   - In the **Select or enter a database name** list, select the name of your Configuration Manager site database.
5. To verify the database connection, click **Test Connection**.
6. If the connection succeeds, click **OK** to close the **Connection Manager** dialog box. If the connection does not succeed, verify that the information you entered is correct, and then click **Test Connection** again.

7. On the **Select how to define the connection** page, verify that **Create a data source based on an existing or new connection** is selected, verify that the data source you have just specified is selected in the **Data connections** list box, and then click **Next**.

8. In **Data source name**, specify a name for the data source and then click **Finish**. For this example, type **Advanced_Model**.

9. The data source **Advanced_Model.ds** is displayed in **Solution Explorer** under the **Data Sources** node.

> **NOTE**
> To edit the properties of an existing data source, double-click the data source in the **Data Sources** folder of the **Solution Explorer** pane to display the data source properties in Data Source Designer.

To define the data source view for the report model

1. In **Solution Explorer**, right-click **Data Source Views** to select **Add New Data Source View**.

2. On the **Welcome to the Data Source View Wizard** page, click **Next**. The **Select a Data Source** page is displayed.

3. In the **Relational data sources** window, verify that the **Advanced_Model** data source is selected, and then click **Next**.

4. On the **Select Tables and Views** page, select the following views in the **Available objects** list to be used in the report model:

   - **v_R_System (dbo)**
   - **v_GS_OPERATING_SYSTEM (dbo)**

   After selecting each view, click **>** to transfer the object to the **Included objects** list.

> **TIP**
> To help locate views in the **Available objects** list, click the **Name** heading at the top of the list to sort the objects in alphabetical order.

5. If the **Name Matching** dialog box appears, accept the default selections, and click **Next**.

6. When you have selected the objects you require, click **Next**, and then specify a name for the data source view. For this example, type **Advanced_Model**.

7. Click **Finish**. The **Advanced_Model.dsv** data source view is displayed in the **Data Source Views** folder of **Solution Explorer**.

To define relationships in the data source view

1. In **Solution Explorer**, double-click **Advanced_Model.dsv** to open the Design window.

2. Right-click the title bar of the **v_R_System** window to select **Replace Table**, and then click **With New Named Query**.

3. In the **Create Named Query** dialog box, click the **Add Table** icon (typically the last icon in the ribbon).

4. In the **Add Table** dialog box, click the **Views** tab, select **V_GS_OPERATING_SYSTEM** in the list, and then click **Add**.

5. Click **Close** to close the **Add Table** dialog box.

6. In the **Create Named Query** dialog box, specify the following information:

- **Name:** Specify the name for the query. For this example, type **Advanced_Model**.
- **Description:** Specify a description for the query. For this example, type **Example Reporting Services report model**.

7. In the **v_R_System** window, select the following items in the list of objects to display in the report model:
   - **ResourceID**
   - **ResourceType**
   - **Active0**
   - **AD_Domain_Name0**
   - **AD_SiteName0**
   - **Client0**
   - **Client_Type0**
   - **Client_Version0**
   - **CPUType0**
   - **Hardware_ID0**
   - **User_Domain0**
   - **User_Name0**
   - **Netbios_Name0**
   - **Operating_System_Name_and0**
8. In the **v_GS_OPERATING_SYSTEM** box, select the following items in the list of objects to display in the report model:
   - **ResourceID**
   - **Caption0**
   - **CountryCode0**
   - **CSDVersion0**
   - **Description0**
   - **InstallDate0**
   - **LastBootUpTime0**
   - **Locale0**
   - **Manufacturer0**
   - **Version0**
   - **WindowsDirectory0**
9. To present the objects in these views as one list to the report author, you must specify a relationship between the two tables or views by using a join. You can join the two views by using the object **ResourceID**, which appears in both views.
10. In the **v_R_System** window, click and hold the **ResourceID** object and drag it to the **ResourceID** object in

the **v_GS_OPERATING_SYSTEM** window.

11. Click **OK.**
12. The **Advanced_Model** window replaces the **v_R_System** window and contains all of the necessary objects required for the report model from the **v_R_System** and the **v_GS_OPERATING_SYSTEM** views. You can now delete the **v_GS_OPERATING_SYSTEM** window from the Data Source View Designer. Right-click the title bar of the **v_GS_OPERATING_SYSTEM** window to select **Delete Table from DSV**. In the **Delete Objects** dialog box, click **OK** to confirm the deletion.
13. Click **File**, and then click **Save All**.

To create the report model

1. In **Solution Explorer**, right-click **Report Models** to select **Add New Report Model**.
2. On the **Welcome to the Report Model Wizard** page, click **Next**.
3. On the **Select Data Source View** page, select the data source view in the **Available data source views** list, and then click **Next**. For this example, select **Simple_Model.dsv**.
4. On the **Select report model generation rules** page, do not change the default values, and click **Next**.
5. On the **Collect Model Statistics** page, verify that **Update model statistics before generating** is selected, and then click **Next**.
6. On the **Completing the Wizard** page, specify a name for the report model. For this example, verify that **Advanced_Model** is displayed.
7. To complete the wizard and create the report model, click **Run**.
8. To exit the wizard, click **Finish**.
9. The report model is shown in the Design window.

To modify object names in the report model

1. In **Solution Explorer**, right-click a report model to select **View Designer**. For this example, select **Advanced_Model.smdl**.
2. In the report model Design view, right-click any object name to select **Rename**.
3. Type a new name for the selected object, and then press Enter. For example, you could rename the object **CSD_Version_0** to read **Windows Service Pack Version**.
4. When you have finished renaming objects, click **File**, and then click **Save All**.

To publish the report model for use in SQL Server Reporting Services

1. In **Solution Explorer**, right-click **Advanced_Model.smdl** to select **Deploy**.
2. Examine the deployment status at the lower left corner of the **SQL Server Business Intelligence Development Studio** window. When the deployment has finished, **Deploy Succeeded** is displayed. If the deployment fails, the reason for the failure is displayed in the **Output** window. The new report model is now available on your SQL Server Reporting Services website.
3. Click **File**, click **Save All**, and then close **SQL Server Business Intelligence Development Studio**.

To deploy the custom report model to Configuration Manager

1. Locate the folder in which you created the report model project. For example, %*USERPROFILE*%\Documents\Visual Studio 2008\Projects\<*Project Name*>.
2. Copy the following files from the report model project folder to a temporary folder on your computer:
   - <*Model Name*> **.dsv**

- *<Model Name>* **.smdl**

3. Open the preceding files by using a text editor, such as Notepad.
4. In the file *<Model Name>***.dsv**, locate the first line of the file, which reads as follows:

   <DataSourceView xmlns="http://schemas.microsoft.com/analysisservices/2003/engine">

   Edit this line to read as follows:

   <DataSourceView xmlns="http://schemas.microsoft.com/analysisservices/2003/engine" xmlns:xsi="RelationalDataSourceView">
5. Copy the entire contents of the file to the Windows Clipboard.
6. Close the file *<Model Name>***.dsv**.
7. In the file *<Model Name>***.smdl**, locate the last three lines of the file, which appear as follows:

   ```
   </Entity>
   ```

   ```
   </Entities>
   ```

   ```
   </SemanticModel>
   ```
8. Paste the contents of the file *<Model Name>***.dsv** directly before the last line of the file (**<SemanticModel>**).
9. Save and close the file *<Model Name>***.smdl**.
10. Copy the file *<Model Name>***.smdl** to the folder *%programfiles%*\Microsoft Configuration Manager\AdminConsole\XmlStorage\Other on the Configuration Manager site server.

> **IMPORTANT**
> After copying the report model file to the Configuration Manager site server, you must exit and restart the Configuration Manager console before you can use the report model in the **Create Report Wizard**.

Security and privacy for reporting in System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This topic contains security best practices and privacy information for reporting in System Center Configuration Manager.

Configuration Manager reports display information that is collected during standard Configuration Manager management operations. For example, you can display a report of information that has been collected from discovery or inventory. Reports can also contain the current status information for client management operations, such as deploying software, and checking for compliance.

For more information about any security best practices and privacy information for Configuration Manager operations that might generate data that can be displayed in reports, see Security best practices and privacy information for System Center Configuration Manager.

The data warehouse service point for Configuration Manager

9/11/2019 • 9 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the data warehouse service point to store and report on long-term historical data for your Configuration Manager deployment.

> **NOTE**
> Configuration Manager doesn't enable this optional feature by default. You must enable this feature before using it. For more information, see Enable optional features from updates.

The data warehouse supports up to 2 TB of data, with timestamps for change tracking. The data warehouse stores data by automatically synchronizing data from the Configuration Manager site database to the data warehouse database. This information is then accessible from your reporting service point. Data synchronized to the data warehouse database is kept for three years. Periodically, a built-in task removes data that's older than three years.

Data that is synchronized includes the following from the Global Data and Site Data groups:

- Infrastructure health
- Security
- Compliance
- Malware
- Software deployments
- Inventory details (however, inventory history isn't synchronized)

When the site system role installs, it installs and configures the data warehouse database. It also installs several reports so you can easily search for and report on this data.

Starting in version 1810, you can synchronize more tables from the site database to the data warehouse. This change allows you to create more reports based on your business requirements.

Prerequisites

- The data warehouse site system role is supported only at the top-tier site of your hierarchy. For example, a central administration site or standalone primary site.
- The computer where you install the site system role requires .NET Framework 4.5.2 or later.
- Grant the **Reporting Services Point Account** the **db_datareader** permission on the data warehouse database.
- To synchronize data with the data warehouse database, Configuration Manager uses the computer account of the site system role. This account requires the following permissions:
  - **Administrator** on the computer that hosts the data warehouse database.
  - **DB_Creator** permission on the data warehouse database.
  - Either **DB_owner** or **DB_reader** with **execute** permissions to the top-tier site's database.

- The data warehouse database requires the use of SQL Server 2012 or later. The edition can be Standard, Enterprise, or Datacenter. The SQL Server version for the data warehouse doesn't need to be the same as the site database server.
- The warehouse database supports the following SQL Server configurations:
  - A default or named instance
  - SQL Server Always On availability group
  - SQL Server failover cluster
- If you use distributed views, the data warehouse service point must install on the same server that hosts the central administration site's database.

For more information on SQL Server licensing, see the product and licensing FAQ.

Size the data warehouse database the same as your site database. While the data warehouse is smaller at first, it will grow over time.

Install

Each hierarchy supports a single instance of this role, on any site system of the top-tier site. The SQL Server that hosts the database for the warehouse can be local to the site system role, or remote. The data warehouse works with the reporting services point installed at the same site. You don't need to install the two site system roles on the same server.

To install the role, use the **Add Site System Roles Wizard** or the **Create Site System Server Wizard**. For more information, see Install site system roles. On the **System Role Selection** page of the wizard, select the **Data Warehouse service point** role.

When you install the role, Configuration Manager creates the data warehouse database for you on the instance of SQL Server that you specify. If you specify the name of an existing database, Configuration Manager doesn't create a new database. Instead it uses the one you specify. This process is the same as when you move the data warehouse database to a new SQL Server.

Configure properties

General page

- **SQL Server fully qualified domain name**: Specify the full qualified domain name (FQDN) of the server that hosts the data warehouse service point database.
- **SQL Server instance name, if applicable**: If you don't use a default instance of SQL Server, specify the named instance.
- **Database name**: Specify a name for the data warehouse database. Configuration Manager creates the data warehouse database with this name. If you specify a database name that already exists on the instance of SQL server, Configuration Manager uses that database.
- **SQL Server port used for connection**: Specify the TCP/IP port number used by the SQL Server that hosts the data warehouse database. The data warehouse synchronization service uses this port to connect to the data warehouse database. By default, it uses SQL Server port **1433** for communication.
- **Data warehouse service point account**: Starting in version 1802, set the **User name** that SQL Server Reporting Services uses when it connects to the data warehouse database.

Synchronization schedule page

Applies to version 1806 and earlier

- **Start time**: Specify the time that you want the data warehouse synchronization to start.

- **Recurrence pattern**
  - **Daily**: Specify that synchronization runs every day.
  - **Weekly**: Specify a single day each week, and weekly recurrence for synchronization.

Synchronization settings page

Applies to version 1810 and later

- **Data Synchronization custom setting**: Choose the option to **Select tables**. In the Database tables window, select the table names to synchronize to the data warehouse database. Use the filter to search by name, or select the drop-down list to choose specific groups. Select **OK** when complete to save.

  > **NOTE**
  > You can't remove tables that the role selects by default.

- **Start time**: Specify the time that you want the data warehouse synchronization to start.
- **Recurrence pattern**
  - **Daily**: Specify that synchronization runs every day.
  - **Weekly**: Specify a single day each week, and weekly recurrence for synchronization.

Reporting

After you install a data warehouse service point, several reports become available on the reporting services point for the site. If you install the data warehouse service point before installing a reporting services point, the reports are automatically added when you later install the reporting services point.

> **WARNING**
> Starting in version 1802, the data warehouse point supports alternative credentials. If you upgraded from a previous version of Configuration Manager, you need to specify credentials that SQL Server Reporting Services uses to connect to the data warehouse database. Data warehouse reports don't open until you add credentials.
>
> To specify an account, set the **User name** for the data warehouse service point account in the role properties. For more information, see Configure properties.

The data warehouse site system role includes the following reports, under the **Data Warehouse** category:

- **Application Deployment - Historical**: View details for application deployment for a specific application and machine.
- **Endpoint Protection and Software Update Compliance - Historical**: View computers that are missing software updates.
- **General Hardware Inventory - Historical**: View all hardware inventory for a specific machine.
- **General Software Inventory - Historical**: View all software inventory for a specific machine.
- **Infrastructure Health Overview - Historical**: Displays an overview of the health of your Configuration Manager infrastructure.
- **List of Malware Detected - Historical**: View malware that has been detected in the organization.
- **Software Distribution Summary - Historical**: A summary of software distribution for a specific advertisement and machine.

Site expansion

Before you can install a central administration site to expand an existing standalone primary site, first uninstall the data warehouse service point role. After you install the central administration site, you can then install the site system role at the central administration site.

Unlike a move of the data warehouse database, this change results in a loss of the historic data you have previously synchronized at the primary site. It isn't supported to back up the database from the primary site and restore it at the central administration site.

Move the database

Use the following steps to move the data warehouse database to a new SQL Server:

1. Use SQL Server Management Studio to back up the data warehouse database. Then, restore that database to a SQL Server on the new computer that hosts the data warehouse.

   > **NOTE**
   > After you restore the database to the new server, make sure the database access permissions are the same on the new data warehouse database as they were on the original data warehouse database.

2. Use the Configuration Manager console to remove the data warehouse service point role from the current server.
3. Reinstall the data warehouse service point. Specify the name of the new SQL Server and instance that hosts the restored data warehouse database.
4. After the site system role installs, the move is complete.

Troubleshooting

Log files

Use the following logs to investigate problems with the installation of the data warehouse service point, or synchronization of data:

- **DWSSMSI.log** and **DWSSSetup.log**: Use these logs to investigate errors when installing the data warehouse service point.
- **Microsoft.ConfigMgrDataWarehouse.log**: Use this log to investigate data synchronization between the site database to the data warehouse database.

Set up failure

When the data warehouse service point role is the first one that you install on a remote server, installation fails for the data warehouse.

Workaround

Make sure that the computer on which you install the data warehouse service point already hosts at least one other role.

Synchronization failed to populate schema objects

Synchronization fails with the following message in **Microsoft.ConfigMgrDataWarehouse.log**:

```
failed to populate schema objects
```

Workaround

Make sure that the computer account of the site system role is a **db_owner** on the data warehouse database.

Reports fail to open

Data warehouse reports fail to open when the data warehouse database and reporting service point are on different site systems.

Workaround

Grant the **Reporting Services Point Account** the **db_datareader** permission on the data warehouse database.

Error opening reports

When you open a data warehouse report, it returns the following error:

```
An error has occurred during report processing. (rsProcessingAborted)
Cannot create a connection to data source 'AutoGen__39B693BB_524B_47DF_9FDB_9000C3118E82_'.
(rsErrorOpeningConnection)
A connection was successfully established with the server, but then an error occurred during the pre-login
handshake. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority that is not
trusted.)
```

Workaround

Use the following steps to configure certificates:

1. On the computer that hosts the data warehouse database:

    a. Open IIS, select **Server Certificates**, and then right-click on **Create Self-Signed Certificate**. Then specify the "friendly name" of the certificate name as **Data Warehouse SQL Server Identification Certificate**. Select the certificate store as **Personal**.

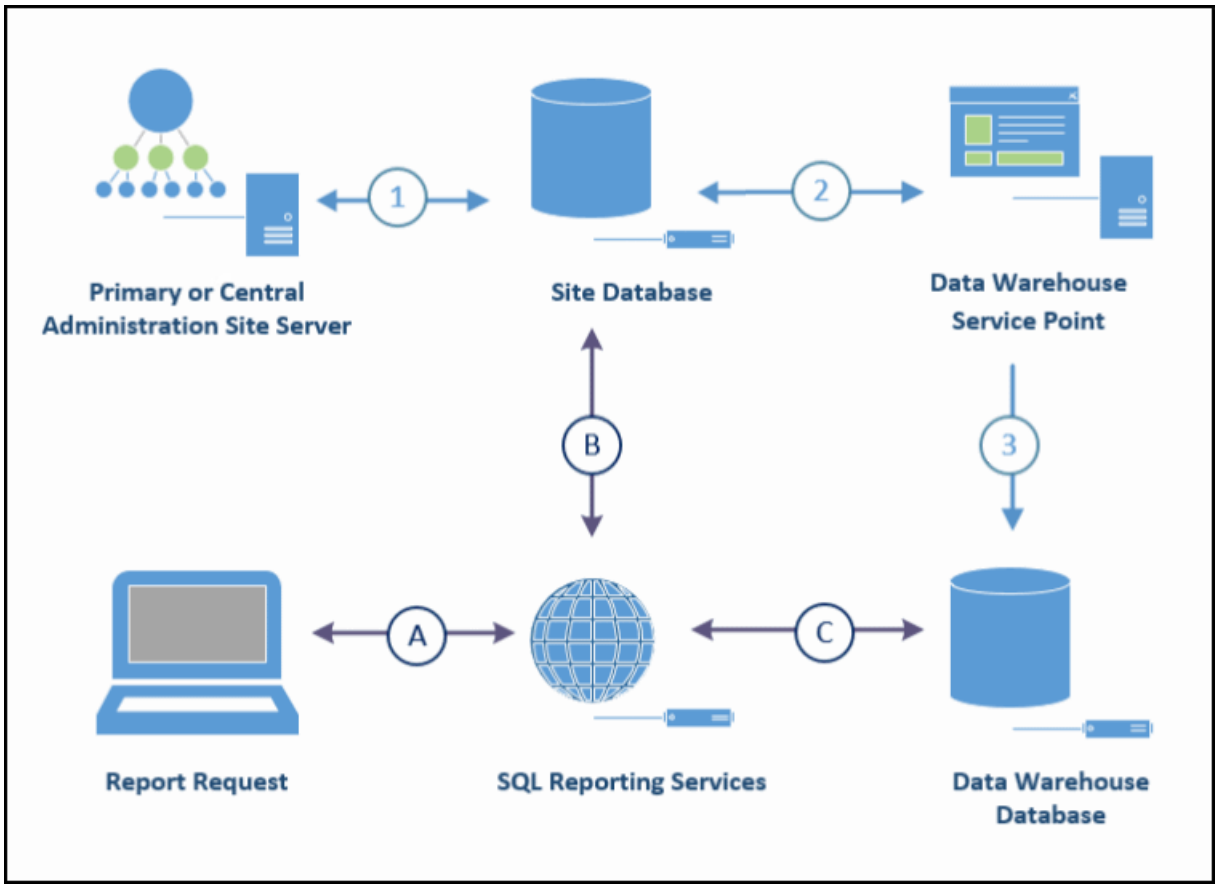
    b. Open **SQL Server Configuration Manager**. Under **SQL Server Network Configuration**, right-click to select **Properties** under **Protocols for MSSQLSERVER**. Switch to the **Certificate** tab, select **Data Warehouse SQL Server Identification Certificate** as the certificate, and then save the changes.

    c. In **SQL Server Configuration Manager**, under **SQL Server Services**, restart the **SQL Server service**. If SQL Reporting Services is also installed on the server that hosts the data warehouse database, restart **Reporting Service** services as well.

    d. Open the Microsoft Management Console (MMC), and add the **Certificates** snap-in. Select **Computer account** of the local machine. Expand the **Personal** folder, and select **Certificates**. Export the **Data Warehouse SQL Server Identification Certificate** as a **DER encoded binary X.509 (.CER)** file.

2. On the computer that hosts SQL Server Reporting Services, open the MMC, and add the **Certificates** snap-in. Select **Computer account**. Under the **Trusted Root Certificate Authorities** folder, import the **Data Warehouse SQL Server Identification Certificate**.

Data flow



Data storage and synchronization

STEP	DETAILS
1	The site server transfers and stores data in the site database.
2	Based on its schedule and configuration, the data warehouse service point gets data from the site database.
3	The data warehouse service point transfers and stores a copy of the synchronized data in the data warehouse database.

Reporting

STEP	DETAILS
A	Using built-in reports, a user requests data. This request is passed to the reporting service point using SQL Server Reporting Services.
B	Most reports are for current information, and these requests are run against the site database.
C	When a report requests historical data by using one of the reports with a *Category* of **Data Warehouse**, the request runs against the data warehouse database.

Support Center for Configuration Manager

7/26/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Starting in version 1810, use Support Center for client troubleshooting, real-time log viewing, or capturing the state of a Configuration Manager client computer for later analysis. Support Center is a single tool to consolidate many administrator troubleshooting tools.

About

Support Center aims to reduce the challenges and frustration when troubleshooting Configuration Manager client computers. Previously, when working with support to address an issue with Configuration Manager clients, you would need to manually collect log files and other information to help troubleshoot the issue. It was easy to accidentally forget a crucial log file, causing additional headaches for you and the support personnel who you're working with.

Use Support Center to streamline the support experience. It lets you:

- Create a troubleshooting bundle (.zip file) that contains the Configuration Manager client log files. You then have a single file to send to support personnel.
- View Configuration Manager client log files, certificates, registry settings, debug dumps, client policies.
- Real-time diagnostic of inventory (replaces ContentSpy), policy (replaces PolicySpy), and client cache.

Support Center viewer

Support Center includes Support Center Viewer, a tool that support personnel use to open the bundle of files that you create using Support Center. Support Center's data collector collects and packages diagnostic logs from a local or remote Configuration Manager client. To view data collector bundles, use the viewer application.

Support Center log file viewer

Support Center includes a modern log viewer. This tool replaces CMTrace and provides a customizable interface with support for tabs and dockable windows. It has a fast presentation layer, and can load large log files in seconds.

Support Center OneTrace (Preview)

Starting in version 1906, **OneTrace** is a new log viewer with Support Center. It works similarly to CMTrace, with improvements. For more information, see Support Center OneTrace.

PowerShell cmdlets

Support Center also includes Windows PowerShell cmdlets. Use these cmdlets to create a remote connection to another Configuration Manager client, to configure the data collection options, and to start data collection.

Prerequisites

Install the following components on the server or client computer on which you install Support Center:

- An OS version supported by Configuration Manager. For more information, see Supported OS versions for clients. Support Center doesn't support mobile devices.
- .NET Framework 4.5.2 is required on the computer where you run Support Center and its components.

Install

Find the Support Center installer on the site server at the following path:
`cd.latest\SMSSETUP\Tools\SupportCenter\SupportCenterInstaller.msi`.

After you install it, find the following items on the Start menu in the **Microsoft System Center** group:

- Support Center (ConfigMgrSupportCenter.exe)
- Support Center Log File Viewer (CMLogViewer.exe)
- Support Center Viewer (ConfigMgrSupportCenterViewer.exe)

Known issues

You can't install the latest version if an older version is already installed

Applies to versions 1810 and 1902

If you already have an older version of Support Center installed, the new installer fails. This issue is due to how the files are versioned between the original version and the latest version. To work around this issue, uninstall the older version of Support Center first. Then install the latest version.

Remote connections must include computer name or domain as part of the user name

If you connect to a remote client from Support Center, you must provide the machine name or domain name for the user account when establishing the connection. If you use a shorthand computer name or domain name (such as `.\administrator`), the connection succeeds, but Support Center doesn't collect data from the client.

To avoid this issue, use the following user name formats to connect to a remote client:

- `ComputerName\UserName`
- `DomainName\UserName`

Scripted server message block connections to remote clients might require removal

When connecting to remote clients using the New-CMMachineConnection PowerShell cmdlet, Support Center creates a server message block (SMB) connection to each remote client. It retains those connections after you complete data collection. To avoid exceeding the maximum number of remote connections for Windows, use the `net use` command to see the currently active set of remote connections. Then disable any unneeded connections by using the following command: `net use <connection_name> /d` where `<connection_name>` is the name of the remote connection.

Application deployment evaluation cycle request isn't sent correctly to remote machines

Applies to version 1810

In Support Center, if you select **Application deployment evaluation** from the **Invoke trigger** action on the **Content** tab, this action starts a task that evaluates deployed applications. If you're connected to a local client, it evaluates both machine and user application deployments. However, if you're connected to a remote client, it only evaluates machine application deployments.

Next steps

Support Center quickstart

Support Center for Configuration Manager

7/26/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Starting in version 1810, use Support Center for client troubleshooting, real-time log viewing, or capturing the state of a Configuration Manager client computer for later analysis. Support Center is a single tool to consolidate many administrator troubleshooting tools.

About

Support Center aims to reduce the challenges and frustration when troubleshooting Configuration Manager client computers. Previously, when working with support to address an issue with Configuration Manager clients, you would need to manually collect log files and other information to help troubleshoot the issue. It was easy to accidentally forget a crucial log file, causing additional headaches for you and the support personnel who you're working with.

Use Support Center to streamline the support experience. It lets you:

- Create a troubleshooting bundle (.zip file) that contains the Configuration Manager client log files. You then have a single file to send to support personnel.
- View Configuration Manager client log files, certificates, registry settings, debug dumps, client policies.
- Real-time diagnostic of inventory (replaces ContentSpy), policy (replaces PolicySpy), and client cache.

Support Center viewer

Support Center includes Support Center Viewer, a tool that support personnel use to open the bundle of files that you create using Support Center. Support Center's data collector collects and packages diagnostic logs from a local or remote Configuration Manager client. To view data collector bundles, use the viewer application.

Support Center log file viewer

Support Center includes a modern log viewer. This tool replaces CMTrace and provides a customizable interface with support for tabs and dockable windows. It has a fast presentation layer, and can load large log files in seconds.

Support Center OneTrace (Preview)

Starting in version 1906, **OneTrace** is a new log viewer with Support Center. It works similarly to CMTrace, with improvements. For more information, see Support Center OneTrace.

PowerShell cmdlets

Support Center also includes Windows PowerShell cmdlets. Use these cmdlets to create a remote connection to another Configuration Manager client, to configure the data collection options, and to start data collection.

Prerequisites

Install the following components on the server or client computer on which you install Support Center:

- An OS version supported by Configuration Manager. For more information, see Supported OS versions for clients. Support Center doesn't support mobile devices.
- .NET Framework 4.5.2 is required on the computer where you run Support Center and its components.

Install

Find the Support Center installer on the site server at the following path: `cd.latest\SMSSETUP\Tools\SupportCenter\SupportCenterInstaller.msi`.

After you install it, find the following items on the Start menu in the **Microsoft System Center** group:

- Support Center (ConfigMgrSupportCenter.exe)
- Support Center Log File Viewer (CMLogViewer.exe)
- Support Center Viewer (ConfigMgrSupportCenterViewer.exe)

Known issues

You can't install the latest version if an older version is already installed

Applies to versions 1810 and 1902

If you already have an older version of Support Center installed, the new installer fails. This issue is due to how the files are versioned between the original version and the latest version. To work around this issue, uninstall the older version of Support Center first. Then install the latest version.

Remote connections must include computer name or domain as part of the user name

If you connect to a remote client from Support Center, you must provide the machine name or domain name for the user account when establishing the connection. If you use a shorthand computer name or domain name (such as `.\administrator`), the connection succeeds, but Support Center doesn't collect data from the client.

To avoid this issue, use the following user name formats to connect to a remote client:

- `ComputerName\UserName`
- `DomainName\UserName`

Scripted server message block connections to remote clients might require removal

When connecting to remote clients using the New-CMMachineConnection PowerShell cmdlet, Support Center creates a server message block (SMB) connection to each remote client. It retains those connections after you complete data collection. To avoid exceeding the maximum number of remote connections for Windows, use the `net use` command to see the currently active set of remote connections. Then disable any unneeded connections by using the following command: `net use <connection_name> /d` where `<connection_name>` is the name of the remote connection.

Application deployment evaluation cycle request isn't sent correctly to remote machines

Applies to version 1810

In Support Center, if you select **Application deployment evaluation** from the **Invoke trigger** action on the **Content** tab, this action starts a task that evaluates deployed applications. If you're connected to a local client, it evaluates both machine and user application deployments. However, if you're connected to a remote client, it only evaluates machine application deployments.

Next steps

Support Center quickstart

Support Center quickstart guide

7/19/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Support Center has powerful capabilities including troubleshooting and real-time log viewing. It can also be used in just a few minutes to capture the state of a Configuration Manager client computer. This ability includes accessing remote clients.

Create a complete *troubleshooting bundle* file (.zip) that captures the client state. The bundle doesn't only contain log files. It can include other types of data such as registry settings and client configurations. Provide the bundle to a support technician who uses Support Center Viewer.

Prerequisites

- Local administrative rights to a Configuration Manager client
- The Support Center installer. This file is on the site server at `cd.latest\SMSSETUP\Tools\SupportCenter\SupportCenterInstaller.msi`. For more information, see Support Center - Install.

Step 1: Create a data bundle on a local client

1. Install Support Center on the Configuration Manager client.
2. Go to the **Start** menu, in the **Microsoft System Center** group, select **Support Center**.
3. On the Home tab of the ribbon, select **Collect Selected Data**. By default, Support Center only collects the minimum data set: log files, client configuration, and operating system.
4. Save the troubleshooting bundle file (.zip) to a folder on the computer. By default, the file name is similar to the following example: `Support_c885cdfed3c7482bba4f9e662978ec07.zip`.

Step 2: View the data bundle using Support Center Viewer

1. Start **Support Center Viewer**. This action can happen on any computer on which you install Support Center.
2. Select **Open bundle**, browse to the bundle file, and select **Open**.
3. After Support Center Viewer processes the file, switch to each available tab. View the types of data that Support Center collects by default:
   - **Configuration**
     - Configuration Manager client configuration
     - Operating system
     - Computer
     - Services
     - Network adapters
   - **Logs**: Choose one or more entries in the list, and select **Open**. This action opens the selected log files

in Log Viewer. Use this feature to look up error codes, and use advanced filters to help you more quickly analyze log files.

Collect more data

Beyond these basic capabilities, Support Center can also collect a wide variety of other client state information. Open **Support Center** and select **Collect All Data**. This process typically lasts several minutes, even on newer computers. Support Center collects the following additional data:

- **Policy**: Configuration Manager policy settings, including both the requested policy configuration and the actual policy configuration
- **Certificates**: Public key information for client certificates. Support Center doesn't collect certificate private keys.
- **Client registry**: Collects client configuration information from the registry. Support Center only collects Configuration Manager registry information.
- **Client WMI**: Client configuration information from WMI. Support Center doesn't collect client policy.
- **Troubleshooting**: Real-time troubleshooting data to help diagnose common client problems with Active Directory, management points, networking, policy assignments, and registration.
- **Debug dumps**: Perform debug dump of client and related processes. Debug dumps can be large. Only enable this option when troubleshooting issues with client performance.

Accessibility features in Support Center

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Support Center has many helpful accessibility features that make it easier for everyone to use.

Use the keyboard to move around the ribbon

Use keyboard shortcuts to access every menu of the Support Center ribbon. This ribbon contains all commands used by Support Center.

1. Press **Alt** or **F10** to see keyboard shortcuts for each menu.
2. To switch to a menu, press the associated shortcut key. For example, to go to the **Logs** menu, press **Alt** and then **L**.

Use the keyboard to perform common tasks

You can also use a keyboard to perform common tasks in Support Center, Support Center Viewer, and Log Viewer. The following table lists the most common tasks that you can perform with the keyboard:

TASK	KEYBOARD SHORTCUT
Open application configuration options	**F4**
Exit	**Alt** + **F4**
Load or Refresh client details (on the Support Center **Client Details** tab)	**F5**
Load selected policy view (on the Support Center **Client Policy** tab)	**F5**
Refresh a policy (on the Support Center **Client Policy** tab, after selecting a policy)	**F5**
Copy as MOF (on the Support Center **Client Policy** tab, after selecting a policy; also available for WMI events)	**Ctrl** + **Shift** + **C**
Copy a policy as local client MOF (on the Support Center **Client Policy** tab, after selecting a policy)	**Ctrl** + **Shift** + **X**
Request policy (on the Support Center **Client Policy** tab)	**Ctrl** + **R**
Evaluate policy (on the Support Center **Client Policy** tab)	**Ctrl** + **E**

TASK	KEYBOARD SHORTCUT
Load or refresh content view (on the Support Center **Content** tab)	**F5**
Load inventory (on the Support Center **Inventory** tab)	**F5**
Start troubleshooting (on the Support Center **Troubleshooting** tab)	**F5**
Open data bundle (on the Support Center Viewer **Home** tab)	**Ctrl** + **O**
Open log files (on the Support Center **Logs** tab, and in the Log Viewer window)	**Ctrl** + **O**
Open log files in current view (on the Support Center **Logs** tab, and in the Log Viewer window)	**Ctrl** + **Shift** + **O**
Open log files in a new Log Viewer window (on the Support Center **Logs** tab, and in the Log Viewer window)	**Ctrl** + **N**
Close all log files (on the Support Center **Logs** tab, and in the **Log Viewer** window)	**Ctrl** + **W**
Search in log files	- **Ctrl** + **F**: Opens the **Find** dialog to enter search string - **F3**: Find the next match - **Shift** + **F3**: Find the previous match
Look up an error code (on **Logs** tab, and in the **Log Viewer** window)	**Ctrl** + **L**
Copy from a log file	- **Ctrl** + **C**: Copies log file text - **Ctrl** + **Shift** + **C**: Copies the log entry without formatting
Quick filter using log file text (on **Logs** tab, and in the **Log Viewer** window)	**Ctrl** + **Shift** + **C**
Annotate a log file (on **Logs** tab, and in the **Log Viewer** window)	**Ctrl** + **Shift** + **N** Note 1
Open Help	**F1**

Note 1: Annotate a log file

Support Center stores annotations in memory. You can only use them within a log viewing session. To retain an annotation for future use, take a screen capture to save the resulting image.

See also

Accessibility features in Configuration Manager

Support Center user interface reference

7/19/2019 • 22 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article is a reference describing the user interfaces (UI) of the Support Center tools:

- Support Center
- Support Center Log Viewer
- Support Center Viewer

Support Center reference

This section describes the user interface for the **Support Center** tool.

Window menu

In the upper left corner of the Support Center window, select the arrow in the blue box to open this menu.

Local Machine Connection

Support Center gathers log files and performs troubleshooting on the client that's running Support Center.

Remote Connection

Establish a remote connection with another Configuration Manager client. After connecting, Support Center gathers log files and performs troubleshooting on the client to which it's connected.

About

Provides information about Support Center.

Options

In the **Options** dialog, you can:

- Reduce the movement of animated user interface elements
- Change the default save location for data bundle files
- Change the location of temporary files
- Reset warnings. Any warning messages that you previously suppressed appear again when triggered.
- Reset temporary file path to the default, `%UserProfile%\AppData\Local\Microsoft\ConfigMgrSupportCenter`

Exit

Close Support Center.

Home tab

Collect selected data

Support Center collects information from the Configuration Manager client. By default, it collects the following

types:

- Log files
- Client configuration collector
- Operating system

To collect other types of information, select the checkbox next to the name for that type.

Select the drop-down at the bottom of the **Collect selected data** button in the ribbon, and select **Collect all data**. This action collects the complete set of client state data.

While Support Center is collecting data, select **Cancel collection** to stop it.

Data types

When you select the checkbox for an option, Support Center collects that type of data the next time you select **Collect selected data**. The following types are available:

- **Log files**: Client log files including setup logs
- **Policy**: Client policy collection
- **Certificates**: Public key information for client certificates. Support Center doesn't collect certificate private keys.
- **Client configuration collector**: Configuration Manager client information. You can't disable this data type.
- **Client registry**: Collects client configuration information from the registry. Support Center only collects Configuration Manager registry information.
- **Client WMI**: Client configuration information from WMI. Support Center doesn't collect client policy.
- **Troubleshooting**: Real-time troubleshooting data to help diagnose common client problems with Active Directory, management points, networking, policy assignments, and registration.

  > **NOTE**
  > This data type isn't supported when you make a remote connection to another client.

- **Debug dumps**: Perform debug dump of client and related processes. Debug dumps can be large. Only enable this option when troubleshooting issues with client performance.

  > **WARNING**
  > Collecting debug dumps will cause data bundles to become very large (in some cases, several hundred MB).
  >
  > Debug dumps contain may contain sensitive information, including passwords, cryptographic secrets, or user data. Debug dumps should only be collected on the recommendation of Microsoft Support personnel. Data bundles that contain debug dumps should be handled carefully to protect them from unauthorized access.
  >
  > This data type isn't supported when you make a remote connection to another client.

- **Operating system**: Collects configuration information about the local machine. This data includes information about the Windows installation, network adapters, and system service configuration. You can't disable this data type.

Client tab

Load or Refresh

Support Center loads or refreshes details for the Configuration Manager client.

Control client agent service

Perform one of the following actions on the Configuration Manager client agent service (ccmexec) on the connected client:

- **Restart client**

  > **IMPORTANT**
  > If the client agent service doesn't successfully restart, the client isn't manageable by Configuration Manager until the service starts.

- **Start client**
- **Stop client**

  > **IMPORTANT**
  > The client isn't manageable by Configuration Manager until the service starts.

Properties

When you load client details, Support Center shows the following properties:

- **Client ID**: A unique identifier that Configuration Manager uses to identify the client
- **Hardware ID**: A unique identifier that Configuration Manager uses to identify the client hardware
- **Approved**: Indicates whether the client is approved in Configuration Manager
- **Registration State**: Indicates whether the client is registered with Configuration Manager
- **Internet-facing**: Indicates whether the client is on the internet
- **Version**: The version number of the installed Configuration Manager client
- **Site Code**: The site code for the primary site to which the client is assigned
- **Assigned MP**: The fully qualified domain name (FQDN) of the client's currently assigned management point
- **Resident MP**: The FQDN of the resident management point
- **Proxy MP**: The hostname or FQDN of the proxy management point (if it exists)
- **Proxy Site Code**: The site code for the secondary site (if it exists)
- **Proxy State**: The state of the Configuration Manager client's proxy management point. For example, **Active** or **Pending**.

Policy tab

Use the actions on this tab instead of the older PolicySpy tool.

Load policy

This option varies depending upon the view:

- **Load Actual policy**: Select **Actual** in the View group, and then select this option in the Policy group. Support Center loads the client policy that you've currently selected.
- **Load Requested policy**: Select **Requested** in the View group, and then select this option in the Policy group. Support Center loads the client policy requested of the client.

- **Load Default policy**: Select **Default** in the View group, and then select this option in the Policy group. Support Center loads the default policy for this client.

Select the drop-down list at the bottom of this button for additional options:

- **Load or Refresh all**: Loads or refreshes the actual, requested, and default policy at the same time.

Actual view

Opens the actual policy view

Requested view

Opens the requested policy view

Default view

Opens the default policy view. (This policy is what devices get when you install the Configuration Manager client.)

Request and evaluate policy

Support Center requests the client policy from the management point, and then evaluates that policy on the client.

Select the drop-down list at the bottom of this button for additional options:

- **Request policy**: Support Center requests the client policy from the management point.
- **Evaluate policy**: Support Center evaluates the client policy on the client.
- **Reset policy to default**: Support Center tells the Configuration Manager client to reapply the default policy. It removes all machine and user policies on the client.

Listen for policy events

Support Center listens for policy events. Select this option again to disable listening for policy events. To view **Policy events**, select the arrow at the bottom of this tab.

Clear events

Support Center clears any policy events.

Content tab

View content on the client, including cached content. Monitor the progress of software update and application deployments.

Load or Refresh

Applies to the Content and Cache views

Support Center loads or refreshes the list of content currently on the client.

Invoke trigger

The following items on this menu request a client action related to content:

- **Location services**
  - **Refresh content locations**: Refreshes the distribution points used by any active content downloads.
  - **Refresh management points**: Updates the internal list of management points used by the client.
  - **Time out content requests**: If any content location requests have been running for too long, this action stops the request.
- **Application deployment evaluation**: Starts a task that evaluates deployed applications.
- **Software updates deployment evaluation**: Starts a task that evaluates deployed software updates.
- **Software updates source scan**: Starts a task that scans update source locations.
- **Windows Installer source list update**: Starts a task that updates the source location for Windows Installer

(MSI) installations.

Content view

See applications, packages, and updates that are loaded on the client. When you select an application, package or update, you can view details on that content. For some applications, you can also do the following actions:

- **Refresh**: Refresh the details view
- **Verify or Download**: Verify that an application is available for download
- **Install**: Install the application
- **Uninstall**: Uninstall the application

Cache view

View the client cache configuration and details about the cache contents. When you connect Support Center to a local client, you ca also do the following actions:

- To change the cache location, select **Change** next to the **Cache location** field.
- To adjust the size of the cache, select **Change** next to the **Cache size** field.
- To clear the client cache, select **Clear** next to the **Cache in use** field.

This view shows the following properties:

- **Location**: The location of each cache folder. Select the link to open the folder in Windows Explorer.
- **Content ID**
- **Cache ID**
- **Size**
- **Last Referenced**: This property is the date when the client last read from or wrote to this item in the cache.

Monitoring view

Select **Monitor** to view the active progress of software update and application update deployments. This view shows state messages raised from application and software updates event WMI messages.

For each event, the view shows the following properties:

- **Time**: The time that the client raised the event
- **Topic type**: The state message type
- **Topic ID**: ID of the state message, used to map to events in log files
- **Topic ID type**: The subtype of the state message
- **State ID**: The result of the action that you're monitoring
- **Details** and **Event data**: More information on the state messages shown in this view. State details may sometimes be blank.

Inventory tab

Load or Refresh

Support Center loads or refreshes the client inventory list for the currently selected view.

Invoke trigger

> **NOTE**
>
> For tasks other than **Software metering report cycle**:
>
> - If you request the task when another inventory task is already running, the client queues the new task to run after it completes the current task and other queued tasks.
> - Track the progress of the task in **InventoryAgent.log**.

The following items on this menu request client action related to inventory:

- **Discovery data collection cycle (heartbeat)**: Triggers the client task used to collect device discovery information
- **File collection cycle**: Triggers the client task used to collect local files
- **Hardware inventory cycle**: Triggers the client task used to collect hardware inventory data
- **IDMIF collection cycle**: Triggers the client task used to collect IDMIF data
- **Software inventory cycle**: Triggers the client task used to collect software inventory data
- **Software metering report cycle**: Triggers the client task used to build a software metering report and send it to the management point. Track the progress of this task in **SWMTRReportGen.log**.
- **Send unsent state messages in queue**: Triggers the client task to flush the queue of state messages.
- **Advanced**
  - **Hardware inventory cycle (full resynchronization)**
  - **Software inventory cycle (full resynchronization)**

Views

If a feature isn't enabled, the view doesn't display any data.

- **Status**: Show the inventory data sets the client has collected
- **DDR**: Information about the client discovery data collected from the client
- **HINV**: Information about the hardware inventory data collected from the client
- **SINV**: Information about the software inventory data collected from the client
- **File collection**: Information about the files collected from the client
- **IDMIF**: Information about the IDMIF and NOIDMIF data collected from the client
- **Metering**: Information about the software metering data collected from the client

Troubleshooting tab

Troubleshoot some of the most common issues with Configuration Manager clients:

- Issues with Active Directory
- Windows networking
- Configuration Manager
  - Management points
  - Policy assignment
  - Registration

> **NOTE**
> This tab isn't available when you connect to a remote Configuration Manager client.

Start

Starts troubleshooting the client

- **Active Directory**: Queries Active Directory to retrieve published Configuration Manager site information
- **MPCERTIFICATE**: Gets management point certificates

- **MPLIST**: Gets a list of management points
- **MPKEYINFORMATION**: Gets management point cryptographic key information
- **Networking**: Troubleshoots issues with networking
- **Policy Assignments**: Retrieves policy assignments
- **Registration**: Verifies that the client is registered with the site

View selected log

After you select a row on the Troubleshooting tab, select this action to view the log file.

Keep previous results

If you troubleshoot the client, and then want to try troubleshooting again, choose this option to retain results from your first attempt. Otherwise, Support Center overwrites previous troubleshooting log files.

Logs tab

This section lists the items on the **Logs** tab of the Support Center tool.

This tab is almost identical to the **Log Viewer** tool. The **Log Viewer** tool doesn't include the **Configure client logging** and **Log groups** features described in this section. The Support Center Log Viewer reference section details the other options available on this tab.

Configure client logging

Set the following options:

- **Client log level**: Log verbosity and file size
- **Maximum file count**: Allow more than one log file of a given type
- **Maximum file size**: The size in bytes of any given log file before the client creates a new log

> **NOTE**
> If you set these values too low, the client may not log any useful information. If you set these values too high, the client logs can consume large amounts of storage.

Log groups

Instead of manually selecting log files using the **Open logs** button, use this drop-down list to open all log files associated with the following feature areas:

- **Desired Configuration Management**
- **Inventory**
- **Software Distribution**
- **Software Updates**
- **Application Management**
- **Policy**
- **Client Registration**
- **Operating System Deployment**

Support Center Log Viewer reference

This section describes the user interface for the **Support Center Log Viewer** tool.

- Window menu
- Home tab

The **Log Viewer** tool is almost identical to the **Logs** tab of **Support Center**. The **Log Viewer** tool doesn't include the options to **Configure client logging** and **Log groups**.

Window menu

In the upper left corner of the Support Center Log Viewer window, select the arrow in the blue box to open this menu.

Open logs

Browse to the location of log files to open.

Options

In the **Options** dialog, you can:

- Reduce the movement of animated user interface elements
- Register Log Viewer as the default app for log files with the .log and .lo_ file extensions
- Reset warnings. Any warning messages that you previously suppressed appear again when triggered.

About

Displays information about Support Center Log Viewer

Close

Closes Support Center Log Viewer

Home tab

Open logs

Support Center prompts you to select one or more log files to open.

Select the drop-down at the bottom of the **Open logs** button in the ribbon, and select one of the following additional options:

- **Open logs in current view**: Opens the selected log files in the current view
- **Open logs in new window**: Opens the selected log files in a new **Log Viewer** window

Close and clear logs

Closes any open log files. Also clears any displayed log file entries from the window. Support Center won't display these entries in the future.

Select the drop-down at the bottom of the **Close and clear logs** button in the ribbon, and select one of the following additional options:

- **Clear all entries**: Clears any displayed log file entries from the window. Support Center won't display these entries in the future.
- **Close all logs**: Closes any open log files

Find

Opens the **Find** dialog. Enter a string to search for. To avoid matches on short strings in other strings, you can choose to match whole words. You can also choose to do a case-sensitive match for the string.

Find next

After finding a match for the string that you're searching for, this option takes you to the next match.

Find previous

After finding two or more matches for the string that you're searching for, this option takes you to the previous match.

Options

- **Live updating**: Monitor a currently open log file for changes. This feature doesn't function when multiple log files are open. This option is enabled by default.
- **Auto-scroll**: If you also chose the **Live updating** option, this option automatically scrolls the log view to show newly added entries. This feature doesn't function when multiple log files are open. This option is enabled by default.

- **Show details**: When you select a log file message, the bottom of the **Logs** tab displays the details of the log file message. This option is enabled by default.
- **Quick filter**: Filter the log file messages across all open log files to find a specific string. You can filter by log text, component name, and thread ID. To find similar log messages, right-click a log message and select **Quick filter** on log text.
- **Wrap log text**: Wrap long and multi-line messages to fit into a single column. This behavior makes these messages easier to read. This option is enabled by default.
- **Raw log entry display**: Displays unprocessed log lines.
- **Advanced filters**: Open the **Advanced filters** dialog. For more information, see Advanced log file filters.
- **Error code links**: Error codes in log text are highlighted and clickable. This option is enabled by default.

Error lookup

Enter an error code to search for that error code in currently open log files. Use the following error code formats:

- **32-bit integer (signed)**: For example, `-2147024891`
- **32-bit integer (unsigned)**: For example, `2147942405`
- **32-bit hexadecimal**: For example, `0x80070005`

Decode certificate

In the **Decode certificate** dialog box, paste the serialized certificate value for any certificate on the client. Find this value in the registry, in log files, or in WMI. Select **Process** to view general information and details on the certificate. This information includes its certification path. Select **Export** to export the certificate as a **.cer** file.

Advanced log file filters

Advanced log file filters allow you to include, exclude, or highlight specific strings. These strings can occur in a log file or log file group when looking at log file entries. Use wildcard searches when creating a filter. When you have a useful combination of filters, save them as a *filter set*.

Advanced log file filters supersede quick filters. Use both together, but quick filters only apply to the displayed log data. Advanced filters determine what data is initially displayed before any it applies any quick filters.

In the Advanced filters dialog, you can create complex filter sets. These filter sets search for strings across many log file components. These components include messages, threads, logging levels, and components. A filter set contains multiple filter statements that you use to include, exclude, or highlight log file messages. A filter defines a log file column to search within, an operator, and a value. The value can contain regular expressions, such as the *wildcard* character `*`.

Add a filter

1. In the **Log Viewer** window, or on the Support Center **Logs** tab, select **Advanced filters**.
2. In the Advanced filters dialog, select **Add**. Then select one of the following options to act on log entries that match your filter:
   - **Include**
   - **Exclude**
   - **Highlight**
3. In the **Advanced filter configuration** dialog, choose a column and an operator:
   - **Column**: Choose where to look for strings that match your filter:
     - **Log text**: Search within the text of a log file

    - **Log severity**: Search for logs with a specific severity level. Set these severity levels in the **Value** field.
    - **Component**: Search for a specific component by name
    - **Thread ID**: Search for log messages with a specific thread ID
    - **Source file**: Search for log messages that occur in a specific log file
  - **Operator**: Choose an operator for your filter
4. Enter a value to filter on in the **Value** field. If your value contains regular expressions, select **Enable regular expression matching**.

Manage filter sets

- To edit a filter, select the filter, and then select**Edit**.
- To delete a filter, select the filter, and then select**Delete**.
- To clear all filters, select **Clear**.
- To save the current filter set, select **Save filters**. Then save your filter set as a **.filterset** file.
- To load a saved filter set, select **Load filters**. Then browse to a previously saved **.filterset** file.

Support Center Viewer reference

This section describes the user interface (UI) for the Configuration Manager **Support Center Viewer** tool. The available tabs vary based on the contents of the troubleshooting bundle. The Window menu and Home tab show by default.

- Window menu
- Home tab
- Configuration tab
- Logs tab
- Debug dumps tab
- WMI tab
- Registry tab
- Policy tab
- Certificates tab
- Troubleshooting tab

Window menu

In the upper left corner of the Support Center Viewer window, select the arrow in the blue box to open this menu.

Open bundle

Browse to the location of a data bundle created by Support Center.

About

Displays information about Support Center Viewer.

Options

In the **Options** dialog, you can:

- Reduce the movement of animated user interface elements
- Change the location of temporary files
- Reset warnings. Any warning messages that you previously suppressed appear again when triggered.
- Reset temporary file path to the default, `%UserProfile%\AppData\Local\Microsoft\ConfigMgrSupportCenterViewer`

Exit

Exits Support Center Viewer

Home tab

Open bundle

Browse to the location of a data bundle created by Support Center.

Open log file

Select one or more log files to open.

Decode certificate

In the **Decode certificate** dialog box, paste the serialized certificate value for any certificate on the client. Find this value in the registry, in log files, or in WMI. Select **Process** to view general information and details on the certificate. This information includes its certification path. Select **Export** to export the certificate as a **.cer** file.

Configuration tab

The **Configuration** tab of the Support Center Viewer tool provides the following views using data retrieved from WMI providers:

Client

This view displays the same information shown on the **Client** tab of Support Center.

Operating system

Details for the client's operating system. It uses the Win32_OperatingSystem class.

Computer

Details for the client computer. It uses the Win32_OperatingSystem class.

Services

Details for services running on the client computer. It uses the Win32_Service class.

Network adapters

Details for network adapters installed on the client computer. It uses the Win32_NetworkAdapterConfiguration class.

Logs tab

The **Logs** tab shows a list of the log files included in the bundle. Each row on this tab provides the path, name, and size of the log file.

Open

After selecting a log file, select this button to open the **Log Viewer**. It provides a subset of the functionality seen on the Support Center Logs tab.

Decode certificate

In the **Decode certificate** dialog box, paste the serialized certificate value for any certificate on the client. Find this value in the registry, in log files, or in WMI. Select **Process** to view general information and details on the certificate. This information includes its certification path. Select **Export** to export the certificate as a **.cer** file.

Debug dumps tab

Each row on this tab provides details on the debug dump files that are available to export. Use this tab to export debug dump files (.dmp) for further analysis. This analysis uses a debugging tool such as WinDbg.

> **WARNING**
>
> Debug dumps may contain sensitive information, including passwords, cryptographic secrets, or user data. Only collect debug dumps on the recommendation of Microsoft Support personnel. Data bundles that contain debug dumps should be handled carefully to protect them from unauthorized access.

Export

Save a copy of the selected debug dump file.

WMI tab

This tab shows the set of WMI data from the Configuration Manager client that the data bundle includes.

Find

Opens the Find dialog, which has the following features:

- **Find what**: Enter a string to search for in the WMI data set. It supports wildcard characters.
- **Look at**: Choose whether you want to search within the WMI data set for a matching **Class or instance name**, **Property**, or **Value**.
- **Match whole string only**: By default, the find dialog searches for strings that contain the string for which you're looking. Choose this checkbox to only find strings that are an exact match to the string that you provided.

Find next

This button opens the next instance of the string that you provided in the Find dialog within the WMI data set.

Decode certificate

In the **Decode certificate** dialog box, paste the serialized certificate value for any certificate on the client. Find this value in the registry, in log files, or in WMI. Select **Process** to view general information and details on the certificate. This information includes its certification path. Select **Export** to export the certificate as a **.cer** file.

Registry tab

Use the **Registry** tab to view registry data included in the data bundle, and to export that data for further analysis.

Export

Save a copy of the registry key and subkeys that you select as a registry (.reg) file.

Find

Opens the Find dialog, which has the following features:

- **Find what**: Enter a string to search for in the WMI data set. It supports wildcard characters.
- **Look at**: Choose whether you want to search within the WMI data set for a matching **Class or instance name**, **Property**, or **Value**.
- **Match whole string only**: By default, the find dialog searches for strings that contain the string for which you're looking. Choose this checkbox to only find strings that are an exact match to the string that you provided.

Find next

This button opens the next instance of the string that you provided in the Find dialog within the WMI data set.

Decode certificate

In the **Decode certificate** dialog box, paste the serialized certificate value for any certificate on the client. Find this value in the registry, in log files, or in WMI. Select **Process** to view general information and details on the certificate. This information includes its certification path. Select **Export** to export the certificate as a **.cer** file.

Policy tab

The **Policy** tab is used to view policy data included in the data bundle.

Find

Opens the Find dialog, which has the following features:

- **Find what**: Enter a string to search for in the WMI data set. It supports wildcard characters.
- **Look at**: Choose whether you want to search within the WMI data set for a matching **Class or instance**

name, **Property**, or **Value**.

- **Match whole string only**: By default, the find dialog searches for strings that contain the string for which you're looking. Choose this checkbox to only find strings that are an exact match to the string that you provided.

Find next

This button opens the next instance of the string that you provided in the Find dialog within the WMI data set.

Decode certificate

In the **Decode certificate** dialog box, paste the serialized certificate value for any certificate on the client. Find this value in the registry, in log files, or in WMI. Select **Process** to view general information and details on the certificate. This information includes its certification path. Select **Export** to export the certificate as a **.cer** file.

Certificates tab

The **Certificates** tab is used to view certificates included in the data bundle, and to export them.

View certificate

Displays information about a selected certificate.

Export

Opens a **Save As** dialog to save a copy of the certificate that you select.

Troubleshooting tab

Use the **Troubleshooting** tab to view log files created using the Support Center Troubleshooting tab.

View log

After you select a row on the **Troubleshooting** tab, select this option to view the log file with Log Viewer.

Customize Support Center

7/19/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The Support Center tool includes a configuration file that you can customize. By default, when you install Support Center, this file is in the following path: `C:\Program Files (x86)\Configuration Manager Support Center\ConfigMgrSupportCenter.exe.config`. The configuration file changes the behavior of the program:

- Customize data collection: Edit the sets of registry keys and WMI namespaces that it includes during data collection
- Customize log groups: Define new groups of log files using regular expressions. Also add other log files to log groups.
- Collect additional log files using wildcards: Use wildcard searches to collect additional log files

To make these changes, you need local administrative permissions on the client where you've installed Support Center. Make these customizations using a text or XML editor, such as Notepad or Visual Studio.

> **IMPORTANT**
> The Support Center configuration file is an XML-formatted file. It's essential to the operation of Support Center. Modifying this file is only recommended for users who are familiar with XML and regular expressions.

Before you customize the Support Center configuration file, save a backup of the original. This backup allows you to recover the original Support Center functionality if you make mistakes while editing the file. If you don't create a backup, and Support Center doesn't function correctly after you modify the configuration file, reinstall Support Center. You can also copy a configuration file from another installation of Support Center.

Customize data collection

To customize the collection of data on the client, modify the Support Center configuration file using XML elements contained within the `<dataCollectorSettings>` element.

WMI data collection

The `<CcmWmiDataCollector>` element contains a `<collectionScopes>` element. Use this element to change the WMI namespaces from which Support Center collects data. It also includes an `<ignoreScopes>` element. Use this element to filter out the collection of data from portions of the namespaces defined in the `<collectionScopes>` element.

Example

The default configuration file collects data from the `root\ccm` namespace. It includes this path in an `<add/>` element in `<collectionScopes>`.

It also ignores everything under the `\cimodels`, `\invagt`, `\events`, and `\policy` paths for this namespace. It includes these paths in `<add/>` elements contained within `<ignoreScopes>`.

```
<CcmWmiDataCollector>
  <collectionScopes>
    <!-- Collect these namespaces (ignoring the sub-scopes in the ignoreScopes block) -->
    <add key="root\ccm"/>
    <add key="root\cimv2\sms"/>
  </collectionScopes>
  <ignoreScopes>
    <!-- Collecting these namespaces is known to be problematic/unnecessary -->
    <add key="root\ccm\cimodels"/>
    <add key="root\ccm\invagt"/>
    <add key="root\ccm\events"/>
    <!-- Do not collect policy, there's already a separate policy collector.-->
    <add key="root\ccm\policy"/>
  </ignoreScopes>
</CcmWmiDataCollector>
```

Registry data collection

The `<RegistryDataCollector>` element contains a `<registryKeys>` element. Use this element to change the registry keys and subkeys that Support Center collects under the `HKEY_LOCAL_MACHINE` path. Support Center doesn't support the collection of registry data from other root registry paths.

Example

To collect registry keys for the classic programs installed on the device, add the following `<add/>` element in the `<registryKeys>` element: `<add key="software\\microsoft\\windows\\currentversion\\uninstall"/>`

```
<RegistryDataCollector>
  <registryKeys>
    <!-- Registry keys (and all subkeys) to collect -->
    <add key="software\\microsoft\\ccm"/>
    <add key="software\\microsoft\\sms"/>
    <add key="software\\microsoft\\ccmsetup"/>
    <add key="software\\microsoft\\windows\\currentversion\\uninstall"/>
  </registryKeys>
</RegistryDataCollector>
```

Customize log file groups

To customize which log files Support Center collects, and how it presents them in the **Log groups** list, use elements in the `<logGroups>` element. When you start Support Center, it scans this section of the configuration file. It then creates a group on the **Log groups** list for each unique key attribute value found in the `<add/>` elements contained in the `<logGroups>` element.

- **Component log group**: The `<componentLogGroup>` element uses a key attribute to define the name of the log group that appears in the list. It also uses a value attribute that contains a regular expression (regex). It uses this regex to collect a set of related log files.
- **Static log group:** The `<staticLogGroup>` element uses a key attribute to define the name of the log group that appears in the list. It also uses a value attribute that defines a log file name.

If the same key attribute value is used in an `<add/>` element within both the `<componentLogGroup>` element and the `<staticLogGroup>` element, Support Center creates a single group. This group includes the log files defined by both elements that use the same key.

Example

```
<logGroups>
  <componentLogGroup>
    <add key="Application Management"
value="^(app.*|ci.*|contentaccess|contenttransfermanager|datatransferservice|dcm.*|execmgr.*|UserAffinity.*|.*H
andler$|.*Provider$)"/>
    <add key="Client Registration" value="^(clientregistration|locationservices|ccmmessaging|ccmexec)"/>
    <add key="Inventory"
value="^(ccmmessaging|inventoryagent|mtrmgr|swmtrreportgen|virtualapp|mtr.*|filesystemfile)"/>
    <add key="Policy" value="^(ccmmessaging|policyagent_.*|policyevaluator_.*)"/>
    <add key="Software Updates"
value="^(ci.*|contentaccess|contenttransfermanager|datatransferservice|dcm.*|update.*|wuahandler|xmlstore|scana
gent)"/>
    <add key="Software Distribution"
value="^(datatransferservice|execmgr.*|contenttransfermanager|locationservices|contentaccess|filebits)"/>
    <add key="Desired Configuration Management" value="^(ci.*|dcm.*)"/>
    <add key="Operating System Deployment" value="^(ts.*)"/>
  </componentLogGroup>
  <staticLogGroup>
    <add key="Application Management" value="ccmsdkprovider.log"/>
    <add key="Desired Configuration Management" value="ccmsdkprovider.log"/>
    <add key="Software Updates" value="ccmsdkprovider.log"/>
  </staticLogGroup>
</logGroups>
```

Collecting additional log files using wildcards

To collect additional log files, use wildcards in the file path or filename. These wildcards include system-wide environment variables such as `%WINDIR%`, but exclude user-scoped environment variables such as `%USERPROFILE%`. To collect additional log files using this non-recursive log file search, use an `<add/>` element within the `<additionalLogFiles>` element.

These examples show how Support Center uses this feature in the default configuration file.

Example 1: Collect all Windows Update log files in the Windows directory

The following element collects any file named `WindowsUpdate.log` found in the Windows directory:

```
<add key="%WINDIR%\WindowsUpdate.log" />
```

Example 2: Collect all log files in the Windows Logs directory

The following element collects any file that ends in `.log` found in the Windows logs directory:

```
<add key="%WINDIR%\logs\*.log" />
```

Full example XML

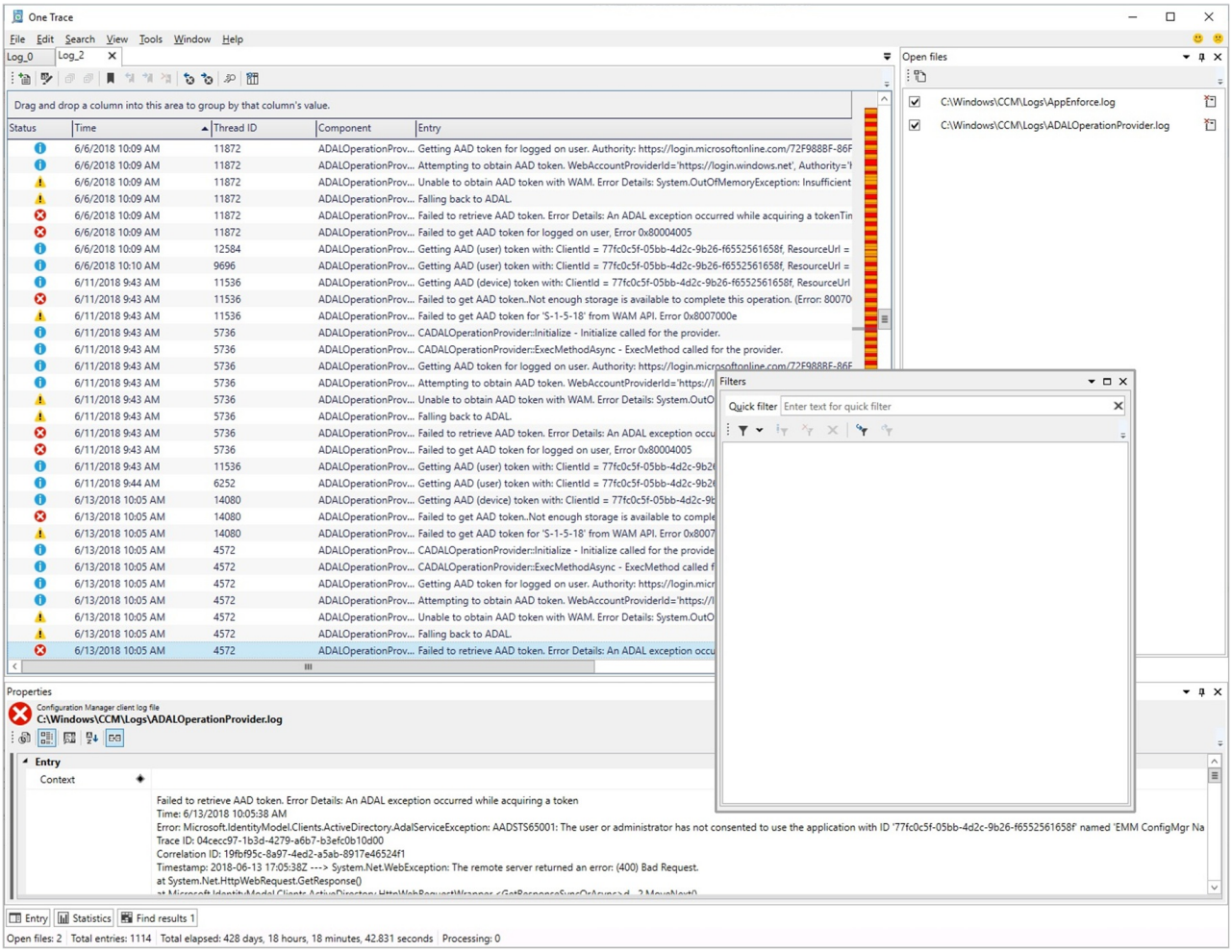
```
<CcmLogDataCollector>
  <additionalLogFiles>
    <!-- Collect these additional log files. Can pass in a wildcard for the filename. System variables are also
supported. -->
    <!--
    <add key="%WINDIR%\WindowsUpdate.log" />
    <add key="%WINDIR%\logs\*.log" />
    -->
  </additionalLogFiles>
</CcmLogDataCollector>
```

Support Center OneTrace (Preview)

7/26/2019 • 2 minutes to read • Edit Online

Starting in version 1906, OneTrace is a new log viewer with Support Center. It works similarly to CMTrace, with the following improvements:

- A tabbed view
- Dockable windows
- Improved search capabilities
- Ability to enable filters without leaving the log view
- Scrollbar hints to quickly identify clusters of errors
- Fast log opening for large files



OneTrace works with many types of log files, such as:

- Configuration Manager client logs
- Configuration Manager server logs
- Status messages
- Windows Update ETW log file on Windows 10
- Windows Update log file on Windows 7 & Windows 8.1

Prerequisites

- .NET Framework version 4.6 or later

Install

OneTrace installs with Support Center. Find the Support Center installer on the site server at the following path: `cd.latest\SMSSETUP\Tools\SupportCenter\SupportCenterInstaller.msi`.

> **NOTE**
> Support Center and OneTrace use Windows Presentation Foundation (WPF). This component isn't available in Windows PE. Continue to use CMTrace in boot images with task sequence deployments.

See also

- Support Center log viewer
- CMTrace

Configuration Manager Tools

9/5/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The Configuration Manager tools include client-based and server-based tools. Use these tools to help support and troubleshoot your Configuration Manager infrastructure.

Starting in Configuration Manager version 1806, these tools are included in the `CD.Latest\SMSSETUP\Tools` folder on the site server. No further installation is required. Use these versions of the tools with Configuration Manager version 1806 and later.

All Windows operating systems listed as supported clients in Supported operating systems for clients and devices are supported for use with these tools.

> **NOTE**
> The System Center 2012 R2 Configuration Manager Toolkit is still available from the Microsoft Download Center. For Configuration Manager version 1806 and later, use the versions of the tools in the CD.Latest folder on the site server. Some tools were formerly in the toolkit but not included in version 1806. These legacy tools are no longer supported.

Client tools

- CMTrace: View, monitor, and analyze Configuration Manager log files
- Client Spy: Troubleshoot issues related to software distribution, inventory, and metering
- Deployment Monitoring Tool: Troubleshoot applications, updates, and baseline deployments
- Policy Spy: View policy assignments
- Power Viewer Tool: View status of power management feature
- Send Schedule Tool: Trigger schedules and evaluations of configuration baselines

> **NOTE**
> The ClientTools folder also includes the file Microsoft.Diagnostics.Tracing.EventSource.dll. Several client tools require this library. You can't directly use it.

Server tools

- DP Job Queue Manager: Troubleshoots content distribution jobs to distribution points
- Collection Evaluation Viewer: View collection evaluation details
- Content Library Explorer: View contents of the content library single instance store
- Content Library Transfer: Transfers content library between drives
- Content Ownership Tool: Changes ownership of orphaned packages. These packages exist in the site without an owning site server.
- Role-based Administration and Auditing Tool: Helps administrators audit roles configuration

- Run Meter Summarization Tool: Run metering summarization task and analyze metering data

> **NOTE**
>
> The ServerTools folder also includes the following files:
>
> - AdminUI.WqlQueryEngine.dll
> - Microsoft.ConfigurationManagement.ManagementProvider.dll
> - Microsoft.Diagnostics.Tracing.EventSource.dll
>
> Several server tools require these libraries. You can't directly use them.

Other tools and toolkits

- Support Center: Gather information from clients for easier analysis when troubleshooting.

  Starting in version 1906, **OneTrace** is a new log viewer with Support Center. It works similarly to CMTrace, with improvements. For more information, see Support Center OneTrace.

- Content library cleanup tool: Use **ContentLibraryCleanup.exe** in `CD.Latest\SMSSETUP\TOOLS\ContentLibraryCleanup` to remove orphaned content from a distribution point.
- Hierarchy Maintenance Tool: Use **Preinst.exe** in the `\<SiteServerName>\SMS_<SiteCode>\bin\X64\00000409` shared folder on the site server to pass commands to the hierarchy manager component.
- Update reset tool: Use **CMUpdateReset.exe** in `CD.Latest\SMSSETUP\TOOLS\CMUpdateReset` to fix issues when in-console updates have problems downloading or replicating.
- Service Connection Tool: Use **ServiceConnectionTool.exe** in `CD.Latest\SMSSETUP\TOOLS\ServiceConnectionTool` to keep your site up-to-date when your service connection point is offline.
- Microsoft Deployment Toolkit (MDT): A collection of tools, processes, and guidance for automating desktop and server OS deployments.
- System Center Updates Publisher (SCUP): A stand-alone tool to manage and import custom software updates.
- Security Content Automation Protocol (SCAP) extensions: Analyze and assess your environment for compliance with NIST baselines.
- Package Conversion Manager: Convert legacy packages into applications.

CMTrace

7/26/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

CMTrace is one of the Configuration Manager tools. It allows you to view and monitor log files, including the following types:

- Log files in Configuration Manager or Client Component Manager (CCM) format
- Plain ASCII or Unicode text files, such as Windows Installer logs

The tool helps to analyze log files by highlighting, filtering, and error lookup.

Starting in version 1806, the CMTrace log viewing tool is automatically installed along with the Configuration Manager client. It's added to the client installation directory, which by default is `%WinDir%\CCM\CMTrace.exe`.

> **NOTE**
> CMTrace isn't automatically registered with Windows to open the .log file extension. For more information, see File associations.

Starting in version 1906, **OneTrace** is a new log viewer with Support Center. It works similarly to CMTrace, with improvements. For more information, see Support Center OneTrace.

Usage

Run **CMTrace.exe**. The first time you run the tool, you see a prompt for file association. For more information, see File associations.

You take most actions in CMTrace from the following menus:

- File
- Tools

File menu

The following actions are available in the **File** menu:

- Open
- Open on Server
- Print
- Preferences

The File menu also lists the last eight recent files. Quickly reopen one of these logs by selecting it from the File menu.

Open

Displays the Open dialog box to browse for a log file.

Filter the view for files of the following types:

- Log files (*.log)
- Old log files (*.lo_)

- All files (*.*)

The following two options aren't selected by default:

- **Ignore existing lines**: When selected, CMTrace ignores the existing contents of the selected log file and displays new lines only as they're added. Use this option to monitor only new actions when you don't need the full history of the log file.
- **Merge selected files**: If you enable this option and select more than one log file, CMTrace merges the selected logs in the view. It displays them as if they're a single log file. The merged log updates the same, and supports all other CMTrace features as if it's a single log file.

Open on Server

Browse the Configuration Manager logs folder on a site system computer with the standard Browse dialog box. You can also browse the network for a remote computer.

When you select a remote computer to browse, CMTrace checks for the Configuration Manager share. If it can't find a share with Configuration Manager log files, it displays an error message.

To connect directly to a known computer without browsing, use the Open action. Then enter a server name and share using the UNC format.

Print

Display the standard Windows Print dialog box. This action sends the current log file to a printer. It formats the output according to the settings on the Printing tab of CMTrace Preferences.

Preferences

Configure settings for CMTrace. The following options are available:

- **General** tab
  - **Update Interval**: Controls how often CMTrace checks for changes to log files and loads new lines. By default, this value is 500 milliseconds.
  - **Highlight**: Sets the color that CMTrace uses when highlighting log lines that you choose. By default, this color is basic yellow (Red: 255, Green: 255, Blue: 0).
  - **Columns**: Configures the columns that are visible in the log view and the order in which they appear. By default, it displays Log Text, Component, Date/Time, and Thread.
- **Printing** tab
  - **Columns**: Configure which columns it uses when printing log files and the order in which they appear. By default, it prints the same columns as it displays.
  - **Orientation**: Sets the default print orientation when printing log files. Override this setting in the Print dialog box. By default, it uses Portrait orientation.
- **Advanced** tab
  - **Refresh Interval**: Forces CMTrace to update the log view at a specified interval when loading a large number of lines. By default, this option is disabled with a value of zero.

    > **NOTE**
    > In general, don't modify the **Refresh Interval**. It can significantly increase the amount of time it takes to open large log files.

Tools menu

The following actions are available in the **Tools** menu:

- Find
- Find Next
- Copy to Clipboard
- Highlight
- Filter
- Error Lookup
- Pause
- Show/Hide Details
- Show/Hide Info Pane

Find

Search the open log file for a specified text string.

Find Next

Finds the next matching string, as you previously specified in the Find dialog box.

Copy to Clipboard

Copies the selected lines as plain text to the Windows clipboard. If you're examining Configuration Manager and CCM log files, it copies the columns in the same order as the view. It separates each column by a tab character. Use this action when copying logs into email messages or other documents.

Highlight

Enter a string that CMTrace uses to search the text of each log entry. It then highlights any log text that matches the string you enter.

- The highlight uses the color you specified in Preferences.
- To turn off highlighting, clearing the string from this field.
- If you enter a decimal or hexadecimal number, CMTrace tries to match the value to the Thread column. Use this behavior to highlight the processing of a single thread, without filtering out other threads that might interact with it.
- To compare strings by case, enable the option for **Case sensitive**.

Filter

Show or hide log lines based on the specified criteria. Apply filters to any of the four columns regardless of whether they're visible. These settings apply to each opened log file.

Examples:

- Filter **smsts.log** on entry text containing "the action" or "the group".
- Filter **InventoryAgent.log** where entry text contains "destination".

Error Lookup

Type or paste an error code in either decimal or hexadecimal format to display a description. Possible error sources include: Windows, WMI, or Winhttp.

Pause

Suspend or restart log monitoring. The following use cases are some of the possible reasons to use this action:

- When CMTrace is displaying log file information too quickly
- When you pause log monitoring, the information that CMTrace displays isn't lost if the current file rolls over to a new log
- When you want to stop CMTrace from displaying new data while you examine the log file

Show/Hide Details

Show or hide all columns other than the log text. It also expands the log text column to the width of the window. Use this action when you're viewing logs on a computer with low display resolution. It displays more of the log text.

> **NOTE**
> When viewing plain-text files, CMTrace automatically hides details because they're always empty.

Show/Hide Info Pane

Show or hide the Info pane. Use this action when you're viewing logs on a computer with low display resolution. It displays more logging details.

Log pane

The log pane is at the top of the CMTrace window. It displays lines from log files.

When you select a line, it's temporarily highlighted using the Windows selection color scheme.

Highlighted lines match the criteria you define with the **Highlight** option in the **Tools** menu. The highlight uses the color that you specify in **Preferences**.

CMTrace displays lines with errors using a red background and yellow text color. In CCM-format logs, log entries have an explicit type value that indicates the entry as an error. For other log formats, CMTrace does a case-insensitive search in each entry for any text string matching "error".

It displays lines with warnings using a yellow background. In CCM-format logs, log entries have an explicit type value that indicates the entry as a warning. For other log formats, CMTrace does a case-insensitive search in each entry for any text string matching "warn".

Info pane

The Info pane is at the bottom of the CMTrace window. It includes the following features:

- Details about the currently selected log entry
- A text box that displays the log text
- It displays carriage returns so that formatted text is easier to read
- Easier to read long entries that aren't fully visible in the Log pane

Show or hide the Info pane with the **Show/Hide Info Pane** option on the **Tools** menu. If the Info pane takes up more than half of the log window, CMTrace automatically hides it.

Progress bar

When you first open a log file, CMTrace replaces the Info pane by a progress bar. This progress indicates how much of the existing file contents it's loaded. The progress reaches 100 percent, CMTrace removes the progress bar, and replaces it with the Info pane. When you load large files, this behavior provides you with an indication of how long the load might take.

Status bar

For Configuration Manager-format and CCM-format log files, the status bar displays the elapsed time for the selected log entries. If you select a single entry, the tool displays the time from the first log entry to the selected entry. If you select multiple entries, it calculates the time from the top-most selected entry to the bottom-most selected entry. CMTrace formats this information as follows:

```
Elapsed time is <hours>h <minutes>m <seconds>s <milliseconds>ms (<seconds+milliseconds> seconds)
```

Windows shell integration

CMTrace supports file associations and drag-and-drop.

File associations

CMTrace can associate itself with .log and .lo_ file name extensions. When the program starts, it checks the registry to determine whether it's already associated with these file name extensions. If CMTrace isn't already associated with any file name extensions, you're prompted to associate the file name extensions with CMTrace. If you select **Do not ask me this again**, CMTrace skips this check whenever it's run on this computer.

Drag-and-drop

CMTrace supports basic drag-and-drop functionality. Drag a log file from Windows Explorer into CMTrace to open it.

Other tips

Last Directory registry key

By default, CMTrace saves the last log location that you opened. This behavior is useful on the site server, as it defaults to the logs path every time.

The first time you launch it on a client, it defaults to the current working directory. This location may be the path where you saved CMTrace, or a path like `%userprofile%\Desktop`.

The **Last Directory** value in the registry key `HKEY_CURRENT_USER\Software\Microsoft\Trace32` controls this default location. If you set this value to `%windir%\CCM\Logs` on your clients, then CMTrace opens files in the client log location the first time you run it.

See also

- Log files
- Support Center log file viewer
- Support Center OneTrace

Client Spy

5/9/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Client Spy is one of the Configuration Manager tools. It's a tool for troubleshooting software distribution, inventory, and software metering on Configuration Manager clients.

Most of the information retrieved by the tool pertains to software deployments:

- All current software deployments
- Software distribution history
- The client cache configuration
- Cached items
- Pending required deployments
- Available deployments

It also displays the following inventory information

- The latest inventory cycle date
- The last report date
- Software inventory major and minor versions
- File collection
- Hardware inventory
- IDMIF collection
- Discovery data records (DDRs)

Software metering rules are also displayed.

> **NOTE**
> To improve performance, the tool only collects information for each tab when you select it. Similarly, when you click **Refresh**, it only refreshes the information for the currently displayed tab.

Usage

Tools menu

The following actions are available in the **Tools** menu:

Connect

Retrieve information from a different computer.

- By default, the tool displays information from the current computer.
- Connect using the remote computer name, user name, and password for the account. The tool makes a connection to the IPC$ share on the remote computer. It deletes the connection when either the tool exits or you connect to another computer.
- It requires an account with sufficient credentials to obtain the information.
- If you don't specify a user name and password, Client Spy uses the security context of the currently signed-

in user to attempt to make the connection.

- When you connect to a remote computer, all tabs that are displayed show information from the remote computer.

Software Distribution

Displays the Software Distribution tabs and hides the other tabs. By default, Client Spy displays the Software Distribution tabs.

Inventory

Displays the Inventory tab and hides the other tabs.

Software Metering

Displays the Software Metering tab and hides the other tabs.

Save current tab to file

Saves the information in the currently displayed tab to a text file that you specify.

Save all tabs to file

Saves the information in all tabs to a text file that you specify. It only saves information your account can see.

Software Distribution tab

Configure settings on the following four tabs:

- Software Distribution Execution Requests
- Software Distribution History
- Software Distribution Cache Information
- Software Distribution Pending Executions

Software Distribution Execution Requests

This tab displays all existing deployments, including both device- and user-targeted deployments.

Each tree item in the Software Distribution Execution Requests tab contains the following four attributes:

- Advertisement ID. This value might be blank, if it's an available deployment.
- Package ID
- Program Name
- User. This might be the targeted user SID or the SID of the user who initiated the request. If both are system requests, the displayed user is System.

For each run request, it also displays the following information in a subtree structure:

- Program Name
- Package ID
- Package Name
- Request Creation Time
- State
- Running State, if State is Running
- Execution Context (User or Admin)
- History State (Success, Failure, or NotRun)
- LastRunTime (Never, if the program hasn't been run before)
- RetryCount, if State is WaitingRetry
- ContentAccess (Retry Count, if State is WaitingRetry)
- FailureCode, if State is WaitingRetry
- FailureReason, if State is WaitingRetry

If the request requires content, the state is WaitingContent. The Software Distribution Cache Information tab shows the details for this download request.

If the run request is a download request, it also displays the number of bytes downloaded.

> **NOTE**
> It uses different icons for varying states of a run request.

Software Distribution History

This tab contains information about all previously run programs. This information is stored in the registry.

The main branches of this tree are the different user histories, including System. It displays a subtree containing the list of packages from which programs have been run for each user.

The package ID and package name for each package subtree displays a list of programs that have run. It displays the following attributes for each:

- Program name
- Run state
- Last run time
- Failure code
- Failure reason

The failure code and failure reason are blank when a program was successfully run.

Software Distribution Cache Information

Cache Config

Contains information about the Configuration Manager Client cache. This information includes the cache location, the cache size, and whether it's currently in use.

Cached Items

Contains a subtree of all items currently in the cache. Each tree item includes the following information about each item:

- The item's location (folder) in the cache
- Current state
- Package ID
- Package name
- Package version
- Package size
- Current reference count
- Last referenced time (UTC)

Downloading Items

These are the items that the client is currently downloading. Each of them shows the same information displayed by the cached items, and the number of kilobytes downloaded.

Software Distribution Pending Executions

This tab contains information that details past and future required deployments and a list of available deployments.

Each tree branch is for each user account with deployments available, including System.

For each user, a sub tree contains the following three items:

Mandatory Advertisements With Future Executions

These are mandatory advertisements that still have programs remaining to be run. These can be either recurring, one-time, or multiple schedule advertisements. Each displays the advertisement ID, the next run time, and the schedule on which the advertisement runs.

Optional Advertisements

Displays a list of all advertisements that are published. It also displays details such as advertisement ID, program name, and package name for each.

Past Mandatory Advertisements With No Future Scheduled Executions

This is a list of advertisements that exist on the client that have no future programs scheduled to run. The advertisement ID, package name, and program name are displayed. A subtree item is displayed for any advertisements that are optional.

> **NOTE**
> Package name information is only available for packages that have advertised policies associated to them on the computer being viewed. Packages that no longer have available policies associated to them display the message "Package Name No Longer Available".

Inventory tab

There's only one tab containing inventory information. The main tree contains the following five items:

- **Software Inventory**: Contains the date that the last cycle started, the date of the last report, and the minor and major versions of the last report.
- **File Collection**: Contains the date that the last cycle started, the date of the last report, and the minor and major versions of the last report.
- **Hardware Inventory**: Contains the date that the last cycle started, the date of the last report, and the minor and major versions of the last report.
- **IDMIF Collection**: Contains the date that the last cycle started, the date of the last report, and the minor and major versions of the last report.
- **DDR**: Contains the date that the last cycle started, the date of the last report, and the minor and major versions of the last report. The DDR information is also displayed in a subtree.

Software Metering tab

This tab displays information as a subtree, and includes all software metering rules. It displays each rule as a node, which it identifies by the file name and rule ID. Expand each node in the tree, and view the following information:

- Explorer file name
- Original file name
- Rule ID
- File version
- Language

Deployment Monitoring Tool

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The Deployment Monitoring Tool is one of the Configuration Manager tools. It's a graphical user interface designed to assist in troubleshooting application, software update, and configuration baseline deployments on a Configuration Manager client. The tool is read-only as it doesn't change any state on the client. You can safely use it to diagnose common deployment scenarios.

Features

- Run it as an administrator to troubleshoot deployments on a local client.
- Troubleshoot deployments on a remote client. Launch the tool and connect to a remote machine as an administrator.
- Export to XML all the data collected in the tool. Share the XML file with others, and use it as a common platform for talking about troubleshooting deployments.
- Import previously exported data to a different machine, and use it to run the tool in offline mode.

Usage

The Deployment Monitoring Tool supports graphical user interface only. To launch the tool, run **DeploymentMonitoringTool.exe** as an administrator. There are three views:

- **Client Properties**: A list of useful attributes about the device and the Configuration Manager client. This view is the default.
- **Deployments**: View all of the currently targeted deployments. Select a deployment in the results pane to view more information in the details pane.
- **All Updates**: View all of the software updates and their status.

To copy data in any view, select a cell, and press **CTRL** + **C**.

Actions menu

The following actions are available in the **Actions** menu:

- **Connect to remote machine**: Select a computer to connect to. When you don't specify a user name and password, it uses the current credentials. Click **Save** to connect to remote computer.
- **Export Data**: Select the file to write the data into, and click **Save**. Use the exported XML file for remote troubleshooting on a different computer.
- **Import Data**: Select a file to import into the tool.
- **View Log**: Opens an associated log file, depending upon the view:
  - Client Properties: `\\<hostname>\c$\Windows\CCM\Logs\PolicyAgent.log`
  - Deployments: `\\<hostname>\c$\Windows\CCM\Logs\PolicyAgent.log`
  - All Updates: `C:\Windows\WindowsUpdate.log`

See also

- Deploy applications
- Deploy software updates
- Deploy configuration baselines

Policy Spy

5/9/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Policy Spy is one of the Configuration Manager tools. It's a tool for viewing and troubleshooting the policy system on Configuration Manager clients. Run **PolicySpy.exe** to open the user interface. For more information on command-line usage, see Command-line syntax.

> **IMPORTANT**
> Run Policy Spy as an administrator. If you don't **Run as administrator**, you see the following error in Client Info:
> `There is no client installed on this machine. Connection to client policy failed with error 80041003`

Command-line syntax

Policy Spy is primarily intended for use through its user interface. It does provide limited command-line options to support automation and batch processing.

```
PolicySpy.exe [/export <ExportFilename> [<computername>]]
```

Option: `/export`

This option silently exports the policy of the local or remote computer. `<ExportFilename>` is the file name to which the tool saves the XML exported policy. If you specify the `<computername>` option, Policy Spy exports the policy of that computer instead of the local computer.

> **NOTE**
> This command-line option doesn't provide a way to specify user credentials. To use alternative credentials to access a remote computer, use the **runas** command to open a new command prompt with the required security credentials.

Usage

Tools menu

The following actions are available in the **Tools** menu:

- **Open Remote**: Connects to the Configuration Manager client policy on a remote computer. Use the Connect dialog box to retrieve the name of the remote computer and optional user credentials. If the connection fails, it displays error information in the Client Info pane. If the connection fails again, try connecting by selecting **Refresh** on the **Edit** menu, or by pressing F5.
- **Open File**: Opens a policy export file (XML) created by the **Export Policy** option. The tool displays the exported policy exactly the same as a live policy. It disables some features that only apply when you connect to an actual client.
- **Request Machine Assignments**: Triggers a request for machine policy assignments on the target computer. This feature is disabled when viewing exported policy.
- **Evaluate Machine Policy**: Triggers a machine policy evaluation on the target computer. This feature is disabled when viewing an exported policy.

- **Request User Assignments**: Triggers a request for user policy assignments for the currently signed-in user. This feature is only available when viewing a policy on the local computer.
- **Evaluate User Policy**: Triggers a user policy evaluation for the currently signed-in user. This feature is only available when viewing a policy on the local computer.
- **Reset Policy**: Removes all non-default policies and resets the policy cookies for the site. It then triggers a request for machine policy assignments. This feature is disabled when viewing an exported policy.
- **Export Policy**: Exports the target computer's policy to an XML file. View this file on any computer with Policy Spy. To open the export file, select **Open File** on the **Tools** menu. This feature is disabled when viewing an exported policy.

Edit menu

The following actions are available in the **Edit** menu:

- **Delete**: Deletes the instance selected in the Results pane. This action is only supported for policy instances. If you try to delete anything other than policy instances, the tool displays an error message. This feature is disabled when viewing an exported policy.
- **Refresh**: Refreshes all results to view the latest information. All tree nodes that are expanded before refreshing are automatically expanded afterward. If Policy Spy hasn't successfully connected to the target computer's policy, it tries to connect again. This feature is disabled when viewing an exported policy.
- **Clear Events**: Clears all items from the Events tab.

Results pane

The results pane displays different views of the policy system on the target computer. Access these views by clicking on one of the following four tabs:

- Actual
- Requested
- Default
- Events

Actual

This tab displays the current policy of the client. The current policy determines a client's behavior and the behavior of its client agents, such as software distribution and inventory. The tab displays results in a tree format with a root node for the computer namespace and each user-specific namespace. Expand a namespace node to display a list of classes. Expand a class to display a list of its instances. The class list includes only classes that have instances.

Requested

This tab displays the policy assignments that the client retrieved from its assigned site. The tab displays results in tree format with a root node for the Machine namespace and each user-specific namespace. Expanding a namespace node displays the following nodes:

- **Configuration**: Displays a list of configuration classes derived from CCM_Policy_Config, which includes policy object, assignments, and others.
- **Settings**: Displays all active settings generated by policies. Settings are displayed under the Configuration node.

> **NOTE**
>
> Multiple instances can exist with the same name because the client hasn't merged these settings into a final resultant set. Policy Spy displays instances under this node by using the RealKey properties instead of their true policy keys. Correlate these instances to the resultant set displayed on the Actual tab.

Default

This tab displays the same information as the **Requested** tab. It also includes contents of the DefaultMachine and DefaultUser namespaces.

Events

This tab displays policy agent events as they happen. The view creates a WMI event subscription for all events derived from CCM_PolicyAgent_Event. The view shows a maximum of 200 events. It removes the oldest events from the top of the list, as necessary. If you select the last item in the list, the list automatically scrolls down as it adds new events. Otherwise, the view maintains its current position, and you must scroll down or press the End key to view new events. This view is always empty when viewing an exported policy.

Client Info pane

The Client Info pane displays a list of properties for the target computer. It displays the following properties, if available:

- Name
- ID
- Version
- Site
- Assigned MP
- Resident MP
- Proxy MP
- Proxy State

Details pane

The Details pane displays detailed information about the current selection. If no selection is active, it displays information about Policy Spy itself, including the version. Otherwise, it displays a Manage Object Format (MOF) representation of the selected item.

Policy Spy uses its own MOF-generation routine to create a more user-friendly HTML display than the plain-text MOF generated by WMI. This behavior allows Policy Spy to add the following features to make the MOF more legible:

- Syntax highlighting
- Indented objects and arrays
- Properties are arranged into system, inherited, and local groups. By default, it collapses the system and inherited groups. You can immediately see which properties the instance actually uses.
- Copy MOF or copy plain-text MOF to the clipboard. This feature is useful for pasting the MOF into other applications by directly calling the MofComp tool.

For instances of Policy objects derived from CCM_Policy_Policy, the details pane displays the policy body below the MOF that displays. If the client hasn't downloaded the policy body, Policy Spy displays a hyperlink. Click the link to download the policy body directly from the client's management point. If the tool successfully downloads the policy

body, it replaces the hyperlink with the contents of the reply. Otherwise, Policy Spy updates the display indicating that the request failed.

Power Viewer Tool

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The Power Viewer tool is one of the Configuration Manager tools. Use it to view the status of the power management feature on a Configuration Manager client.

Run **PowerVwr.exe** as an administrator. When the tool launches, it displays the power capabilities and power settings of the local computer on the **Power Config** tab.

To view the power management data of a remote computer:

1. Go to the **File** menu, and click **Connect**.
2. Enter the **Computer** name, and a **Username** and **Password**, if necessary.

There are three tabs in Power Viewer:

- **Power Config**: View the power capabilities and power settings of the targeted computer.
- **Daily Activity**: View the daily activity charts of the client, which includes the following information:
  - **Computer on**: The power status of the computer in one day. Sleep mode is considered as power off.
  - **Monitor on**: On or off status of monitor in one day.
  - **User Active**: User activity information in one day.
- **Power Events**: View all of the daily power events. The client summarizes these events at 12:00 AM. This summarization generates data for the daily activity chart.

Send Schedule Tool

8/30/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The Send Schedule Tool is one of the Configuration Manager tools. Use it to trigger a schedule on a client or trigger the evaluation of a specified configuration baseline. It works for the local computer or targeting a remote client.

For example, use the tool to trigger an inventory schedule or compliance evaluation. If a number of Configuration Manager clients haven't recently reported inventory or compliance status, run the tool to initiate the necessary schedule on each client.

Usage

Run **SendSchedule.exe** as an administrator.

`SendSchedule /L [Computer Name]` `SendSchedule "<Message GUID | DCM UID>" [Computer Name]`

After you trigger a message (GUID), see **SMSClientMethodProvider.log**. For more information about available message GUIDs, see Message IDs.

After you trigger the evaluation of a configuration baseline (DCM UID), see **DCMAgent.log**.

Command-line options

Option: `/L`

List all Message GUID or DCM UID available for sending. Display the meaningful name of messages in the data table for each one. If the computer name is absent, it uses the local computer. If you specify a message without a machine name, then it sends the message to the local machine.

Examples

List the available messages on the local machine

```
SendSchedule /L
```

List the available messages on the client MyPC:

```
SendSchedule /L MyPC
```

Trigger hardware inventory on the local machine

```
SendSchedule {00000000-0000-0000-0000-000000000001}
```

Trigger hardware inventory on MyPC:

```
SendSchedule {00000000-0000-0000-0000-000000000001} MyPC
```

Trigger the evaluation of a specific configuration baseline on MyPC:

```
SendSchedule ScopeId_611E8382-C064-4B62-B0DE-EFFB52AE8994/Baseline_36722778-69dd-4423-9632-b61148b2b67e MyPC
```

Message IDs

MESSAGE ID	DISPLAY NAME
{00000000-0000-0000-0000-000000000001}	Hardware Inventory
{00000000-0000-0000-0000-000000000002}	Software Inventory
{00000000-0000-0000-0000-000000000003}	Discovery Inventory
{00000000-0000-0000-0000-000000000010}	File Collection
{00000000-0000-0000-0000-000000000011}	IDMIF Collection
{00000000-0000-0000-0000-000000000021}	Request Machine Assignments
{00000000-0000-0000-0000-000000000022}	Evaluate Machine Policies
{00000000-0000-0000-0000-000000000023}	Refresh Default MP Task
{00000000-0000-0000-0000-000000000024}	LS (Location Service) Refresh Locations Task
{00000000-0000-0000-0000-000000000025}	LS Timeout Refresh Task
{00000000-0000-0000-0000-000000000026}	Policy Agent Request Assignment (User)
{00000000-0000-0000-0000-000000000027}	Policy Agent Evaluate Assignment (User)
{00000000-0000-0000-0000-000000000031}	Software Metering Generating Usage Report
{00000000-0000-0000-0000-000000000032}	Source Update Message
{00000000-0000-0000-0000-000000000037}	Clearing proxy settings cache
{00000000-0000-0000-0000-000000000040}	Machine Policy Agent Cleanup
{00000000-0000-0000-0000-000000000041}	User Policy Agent Cleanup
{00000000-0000-0000-0000-000000000042}	Policy Agent Validate Machine Policy / Assignment
{00000000-0000-0000-0000-000000000043}	Policy Agent Validate User Policy / Assignment
{00000000-0000-0000-0000-000000000051}	Retrying/Refreshing certificates in AD on MP
{00000000-0000-0000-0000-000000000061}	Peer DP Status reporting
{00000000-0000-0000-0000-000000000062}	Peer DP Pending package check schedule
{00000000-0000-0000-0000-000000000063}	SUM Updates install schedule
{00000000-0000-0000-0000-000000000101}	Hardware Inventory Collection Cycle
{00000000-0000-0000-0000-000000000102}	Software Inventory Collection Cycle

MESSAGE ID	DISPLAY NAME
{00000000-0000-0000-0000-000000000103}	Discovery Data Collection Cycle
{00000000-0000-0000-0000-000000000104}	File Collection Cycle
{00000000-0000-0000-0000-000000000105}	IDMIF Collection Cycle
{00000000-0000-0000-0000-000000000106}	Software Metering Usage Report Cycle
{00000000-0000-0000-0000-000000000107}	Windows Installer Source List Update Cycle
{00000000-0000-0000-0000-000000000108}	Software Updates Policy Action Software Updates Assignments Evaluation Cycle
{00000000-0000-0000-0000-000000000109}	PDP Maintenance Policy Branch Distribution Point Maintenance Task
{00000000-0000-0000-0000-000000000110}	DCM policy
{00000000-0000-0000-0000-000000000111}	Send Unsent State Message
{00000000-0000-0000-0000-000000000112}	State System policy cache cleanout
{00000000-0000-0000-0000-000000000113}	Update source policy
{00000000-0000-0000-0000-000000000114}	Update Store Policy
{00000000-0000-0000-0000-000000000115}	State system policy bulk send high
{00000000-0000-0000-0000-000000000116}	State system policy bulk send low
{00000000-0000-0000-0000-000000000121}	Application manager policy action
{00000000-0000-0000-0000-000000000122}	Application manager user policy action
{00000000-0000-0000-0000-000000000123}	Application manager global evaluation action
{00000000-0000-0000-0000-000000000131}	Power management start summarizer
{00000000-0000-0000-0000-000000000221}	Endpoint deployment reevaluate
{00000000-0000-0000-0000-000000000222}	Endpoint AM policy reevaluate
{00000000-0000-0000-0000-000000000223}	External event detection

DP Job Queue Manager

5/9/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The Distribution Point (DP) Job Queue Manager is one of the Configuration Manager tools. Use it to troubleshoot and manage ongoing content distribution jobs to Configuration Manager distribution points.

The tool displays the list of jobs that the package transfer manager component has in its queue. It also shows the status of the jobs: ready to be executed, running, or retrying. It lets you manipulate the jobs in the queue, move jobs higher on the list, cancel a job, or manually start running a job.

It also gets information from the site server on which distribution point is running a job. The tool connects through the provider to the site server. It doesn't connect to every remote distribution point to gather this information. Because it triggers actions and gets information through the provider, there's a delay in reflecting changes from remote distribution points.

Usage

Run **DPJobMgr.exe**. The main menu of the tool contains the following tabs:

- Connect: Establish the initial connection to the primary site server
- Overview: Summarizes in a single view all the jobs that are running on all distribution points
- Distribution Point Info: Multi-select distribution points to track them, and manage a single job of interest
- Manage Jobs: Shows in one flat view a list of all the jobs and their statuses. Manipulate jobs, move them up, cancel, or manually start.

Connect tab

Use this tab to establish the initial connection to the primary site server. It uses the currently signed-in user's credentials. You can't connect to the central administration site or secondary sites. The connection requires the **Full Administrator** security role.

Once the tool successfully establishes a connection, a notification at the bottom of the tool confirms that it's connected to the site server.

Overview tab

Shows a summary of all the jobs on all distribution points. See the following columns:

- **Distribution Point**: Lists the names of the distribution points
- **Running Jobs**: Shows the number of concurrent jobs that are running on a particular distribution point.

  > **TIP**
  > The number of concurrent software distributions is a site setting. Modified this setting in the Software Distribution Component Properties.

- **Total Jobs**: Shows the number of all the jobs targeted to a particular distribution point. This number includes the jobs that are running, retrying, or waiting to be executed.
- **Total Retries**: Shows the number of times jobs have been retrying in a particular distribution point. A

higher number may represent a general problem with that particular distribution point.

TIP

- To sort each column in this tab, click on the column name
- Manually refresh the information in this tab by clicking **Refresh**
- Automatically refresh the information in this tab by clicking **Start Auto Refresh** and setting the auto refresh interval. The default refresh interval is two minutes.

Distribution Point Info tab

Shows the list of all the distribution points under the connected site. The pane on the left lists all the distribution points. Click **Select All** or **Unselect All** as necessary, or multi-select specific distribution points in this list. The pane on the right shows the jobs for the selected distribution points.

There are eight columns:

- **Status Icon**: There are three possible status icons:
  - **Ready**: Indicates that a particular job has finished all the verification steps. It's ready to be added to the running concurrent jobs. Jobs in this state are usually in a waiting stage. They wait for the current running processes to finish to open up a space for them.
  - **Running**: Indicates that a particular job is currently running on a distribution point. For long running jobs (large packages), usually there's time to get the progress (%) towards completion. It shows this percentage in the **Progress** column in this view. For small packages, the **Progress** column may stay empty. The job may already be completed by the time it receives status from the remote distribution point.
  - **Retry**: Indicates that a particular job has failed and is now in a retry state. This job is retried after the retry interval. This interval is configurable, and set to 30 minutes by default.
- **Software**: Name of the package that's targeted to a particular distribution point
- **Package ID**: Package ID of the package that's targeted to a particular distribution point
- **Size**: Size of the package in KB
- **Progress**: Job completion percentage. For more information, see the **Running** status icon description.
- **Start/Restart Time**: For a running job, this value is the start time (green). For a retry job, this value is the time that it will retry the job.
- **Retries**: Number of times it has retried this package.
- **Distribution Point Name**: The fully qualified domain name (FQDN) of the distribution point

TIP

- To sort each column in this tab, click on the column name
- Manually refresh the information in this tab by clicking **Refresh**
- Automatically refresh the information in this tab by clicking **Start Auto Refresh** and setting the auto refresh interval. The default refresh interval is two minutes.
- If you need to modify a particular job, right-click the job in this view, and select **Manage Job**. This action opens the Manage Jobs tab.

Manage Jobs tab

Shows in one flat view a list of all the jobs and their statuses. It contains the same eight columns as the Distribution Point Info tab. In this view, right-click the jobs for the following actions:

- **Run**: Starts a job that's in any state other than running
- **Move To Top**: Moves one or more jobs to the top of the queue. This action may result in the jobs running immediately. A lower priority job may pause because of this action.
- **Move Up**: Moves a particular job one row above. A lower priority job may pause running because of this action.
- **Move Down**: Moves a particular job one row below.
- **Move To Bottom**: Moves one or more jobs to the bottom of the queue.

  > **TIP**
  > Drag-and-drop jobs in the list to move them.

- **Cancel**: Tries to cancel one or more jobs.

  > **NOTE**
  > You can't cancel jobs near their final completion time. If the site server is also a distribution point, you can't cancel jobs on the site server.

See also

- Fundamental concepts for content management
- Package transfer manager

Collection Evaluation Viewer

5/9/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Collection Evaluation Viewer is one of the Configuration Manager tools. Use it to view and troubleshoot the collection evaluation process on the primary site server.

The tool displays the following information:

- Both historic and live information for full and incremental collection evaluations
- The evaluation queue status
- The time for collection evaluations to complete
- Which collections are currently being evaluated
- The estimated time that a collection evaluation will start and complete

About collection evaluation

The collection evaluation process runs by evaluating the membership rules of a collection to update its members. The site places a collection that it's evaluating in one of four different queues:

- **Manual Queue**: For collections that an administrator has manually selected for evaluation from the console
- **New Queue**: For newly created collections
- **Full Queue**: For collections due for full evaluation
- **Incremental Queue**: For collections with incremental evaluation

There are four threads that run to evaluate the collections in the above queues. Each queue includes a series of arrays, and each array includes the collections to be evaluated. The thread that's running for the queue selects a collection from the array and runs the evaluation. The queue length indicates the number of arrays in the queue.

Requirements

- Run the tool on the site server
- Run the tool by an administrative user with at least the **Read-Only Analyst** role
- The user also requires **Read** permission to the site database in SQL

Usage

Run **CEViewer.exe**. The main menu of the tool contains the following tabs:

- Connect: Establish the initial connection to the primary site server and SQL Server
- Full Evaluation: Lists the detailed information about all past full evaluations
- Incremental evaluation: Lists the detailed information about all past incremental evaluations
- All Queues: Summarizes the current collection evaluations for all four queues

- Manual Queue: Lists the detailed information about the current collection evaluation in the manual queue
- New Queue: Lists the detailed information about the current collection evaluation in the new queue
- Full Queue: Lists the detailed information about the current collection evaluation in the full queue
- Incremental Queue: Lists the detailed information about the current collection evaluation in the incremental queue

Connect tab

This tab allows you to establish the initial connection to the primary site server. The tool also establishes a connection to the SQL server that hosts the site database.

The connections to both primary site server and SQL servers use the current signed-in user credential. Connections to the central administration site or a secondary site aren't supported. No collection evaluation process runs on those sites.

Once the tool successfully establishes a connection, see a notification at the bottom of the Collection Evaluation Viewer that confirms the tool's connection to the SQL server.

Full Evaluation tab

Shows detailed information about past full collection evaluations. There are eight columns:

- **Collection Name**: Name of the collection
- **Site ID**: Site ID of the collection
- **Run Time**: How long the last collection evaluation ran, in seconds
- **Last Evaluation Completion Time**: When the last collection evaluation completed
- **Next Evaluation Time**: When the next full evaluation starts
- **Member Changes**: The member changes in the last collection evaluation. These changes are either plus (members added) or minus (members removed).
- **Last Member Change Time**: The most recent time that there was a membership change in the collection evaluation
- **Percent**: The percentage of evaluation time for this collection over the total (all collections) evaluation time

Incremental evaluation tab

Shows detailed information about past incremental collection evaluations. There are seven columns:

- **Collection Name**: Name of the collection
- **Site ID**: Site ID of the collection
- **Run Time**: How long the last collection evaluation ran, in seconds
- **Last Evaluation Completion Time**: When the last collection evaluation completed
- **Member Changes**: The member changes in the last collection evaluation. These changes are either plus (members added) or minus (members removed).
- **Last Member Change Time**: The most recent time that there was a membership change in the collection evaluation
- **Percent**: The percentage of evaluation time for this collection over the total (all collections) evaluation time

All Queues tab

Summarizes the live collection evaluations for all four queues. There are six sections:

- **Summary**: Lists the total collection number and the queue length for all collections in all four queues
- **Running Evaluation**: Lists which collection is currently being evaluated in each queue, and how long it has been running
- **Manual Update**: Shows a brief summary of the collections being evaluated, the estimated completion time, and the order of the evaluation in the manual queue
- **New Collection**: Shows a brief summary of the collections being evaluated, the estimated completion time, and the order of the evaluation in the new collection queue
- **Full Evaluation**: Shows a brief summary of the collections being evaluated, the estimated completion time, and the order of the evaluation in the full evaluation queue
- **Incremental Evaluation**: Shows a brief summary of the collections being evaluated, the estimated completion time, and the order of the evaluation in the incremental evaluation queue

Manual Queue tab

Shows information about the manual collection evaluation currently being evaluated. The order in the list is the order in which the collection will be evaluated. There are four columns:

- **Collection Name**: Name of the collection
- **Site ID**: Site ID of the collection
- **Estimated Completion Time**: When the evaluation is estimated to complete
- **Estimated Run Time**: How long the evaluation is estimated to run, in day:hour:minute:second format

New Queue tab

Shows the live information about the new collection evaluation being evaluated. The order in the list is the order in which the collection will be evaluated. There are four columns:

- **Collection Name**: Name of the collection
- **Site ID**: Site ID of the collection
- **Estimated Completion Time**: When the evaluation is estimated to complete
- **Estimated Run Time**: How long the evaluation is estimated to run, in day:hour:minute:second format

Full Queue tab

Shows information about the full collection evaluation currently being evaluated. The order in the list is the order in which the collection will be evaluated. There are four columns:

- **Collection Name**: Name of the collection
- **Site ID**: Site ID of the collection
- **Estimated Completion Time**: When the evaluation is estimated to complete
- **Estimated Run Time**: How long the evaluation is estimated to run, in day:hour:minute:second format

Incremental Queue tab

Shows information about the incremental collection evaluation currently being evaluated. The order in the list is the order in which the collection will be evaluated. There are four columns:

- **Collection Name**: Name of the collection
- **Site ID**: Site ID of the collection
- **Estimated Completion Time**: When the evaluation is estimated to complete

- **Estimated Run Time**: How long the evaluation is estimated to run, in day:hour:minute:second format

Content Library Explorer

5/9/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Content Library Explorer is one of the Configuration Manager tools. Use the tool for the following activities:

- Explore the content library on a specific distribution point
- Troubleshoot issues with the content library
- Copy packages, contents, folders, and files out of the content library
- Redistribute packages to the distribution point
- Validate packages on remote distribution points

Requirements

- Run the tool using an account that has administrative access to:
  - The target distribution point
  - The WMI provider on the site server
  - The Configuration Manager provider
- Only the **Full Administrator** and **Read-Only Analyst** roles have sufficient rights to view all information from this tool.
  - Other roles, such as **Application Administrator**, can view partial information. For more information, see Disabled packages.
  - The **Read-Only Analyst** can't redistribute packages from this tool.
- Run the tool from any computer, as long as it can connect to:
  - The target distribution point
  - The primary site server
  - The Configuration Manager provider
- If the distribution point is colocated with the site server, it's still necessary to have administrative access to the site server.

Usage

When you start **ContentLibraryExplorer.exe**, enter the fully qualified domain name (FQDN) of the target distribution point. It then connects to the distribution point. If the distribution point is part of a secondary site, it prompts you for the FQDN of the primary site server, and the primary site code.

In the left pane, view the packages that are distributed to this distribution point. Expand the packages, and explore their folder structure. This structure matches the folder structure from which you created the package.

When you select a folder, it displays in the right pane any files within the folder. This view includes the following information:

- File name
- File size
- Which drive it's on
- Other packages that use the same file on the drive
- When the file was last changed on the distribution point

The tool also connects to the Configuration Manager provider. This connection is to determine which packages are distributed to the distribution point, and whether they're actually in the distribution point's content library. For instance, a package that's pending distribution may not yet exist in the content library. Such a package would appear as "PENDING" in the tool, and no actions are enabled for this package.

Disabled packages

Some packages are present on the distribution point but not visible in the Configuration Manager console. These packages are marked with an asterisk (*). No actions may be performed on these packages. Other packages may also be marked with an asterisk and have actions disabled.

There are three primary reasons for disabled packages:

- The package is the Configuration Manager client upgrade. This package includes "ccmsetup.exe".
- Your user account can't access the package, likely due to role-based administration. For instance, the **Application Author** role can't see driver packages in the console, so any driver packages on the distribution point are marked as disabled.
- The package is orphaned on the distribution point.

Validate packages

Validate packages by using **Package** > **Validate** on the toolbar. First select a package node in the left pane Don't select a content or a folder. The tool connects to the WMI provider on the distribution point for this action. When the tool starts, packages that are missing one or more contents are marked invalid. Validating the package reveals which content is missing. If all content is present but the data is corrupted, validation detects the corruption.

Redistribute packages

Redistribute packages using **Package** > **Redistribute** on the toolbar. First select a package node in the left pane. This action requires permissions to redistribute packages.

Other actions

Use **Edit** > **Copy** to copy packages, contents, folders, and files out of the content library to a specified folder. You can't copy the content library itself. Select more than one file, but you can't select multiple folders.

Search for packages using **Edit** > **Find Package**. This action searches for your query in the package name and package ID.

Limitations

- The tool can't manipulate the content library directly in any way. Changes to the content library may result in malfunctions.
- The tool can redistribute packages, but only to the target distribution point.
- When you colocate the distribution point with the site server, you can't validate package data. Use the Configuration Manager console instead. The tool still inspects the package to make sure that all the content is present, though not necessarily intact.
- You can't delete content with this tool.

See also

- Fundamental concepts for content management
- The content library

Content Library Transfer tool

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The Content Library Transfer tool is one of the Configuration Manager tools. It transfers content from one disk drive to another. The tool is designed to run on distribution point site systems. It supports distribution points colocated with a site or remote site systems.

The tool is useful for the scenario when the disk drive hosting the content library becomes full. First add or identify another hard disk with sufficient space to host the content library. Then use **ContentLibraryTransfer.exe** to transfer content from the old filled hard disk to the new, empty drive.

Once the transfer is complete, content is accessible to client computers from the new location.

Usage

Run **ContentLibraryTransfer.exe** as a user with administrative permissions on the distribution point.

Syntax

```
ContentLibraryTransfer.exe –SourceDrive <drive letter of source drive> –TargetDrive <drive letter of destination drive>
```

Example

```
ContentLibraryTransfer –SourceDrive E –TargetDrive G
```

Limitations

- Run the tool locally on the distribution point. You can't run it from a remote computer.
- Only use it when clients aren't actively accessing the distribution point. If you run the tool while clients are accessing content, the content library on the destination drive may have incomplete data. The data transfer might fail altogether leading to an unusable content library.
- Don't distribute content to the distribution point when you run the tool. If you run the tool while content is being written to the distribution point, the content library on the destination drive may have incomplete data. The data transfer might fail altogether leading to an unusable content library.

See also

- Fundamental concepts for content management
- The content library

Content Ownership Tool

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Content Ownership Tool is one of the Configuration Manager tools. It changes ownership of orphaned packages in Configuration Manager. Orphaned packages don't have an owning site server. Packages can become orphaned by removing the site server while they're still owned by this site server.

Run the Content Ownership Tool on any site server in the Configuration Manager hierarchy. Sign in as an administrative user with sufficient package permissions.

> **TIP**
> Use **ContentLibraryCleanup.exe** in `CD.Latest\SMSSETUP\TOOLS\ContentLibraryCleanup` to *remove* orphaned content from a distribution point. For more information, see Content library cleanup tool.

Features

- Display all orphaned packages
- Display all packages, even if they're not orphaned
- View the status of the connection to a site
- Filter packages by name, site code, or package type
- Sort by any displayed column
- Change assignment of one or more packages with a single action
- View progress of the ownership transfer activity

Usage

Run **ContentOwnershipTool.exe** to start the tool. Local administrator permissions on the computer aren't required to run the tool.

There are no command-line parameters.

> **IMPORTANT**
> This tool changes the ownership of an orphaned package. The package itself doesn't move from the distribution point that it's stored on. This ownership change doesn't cause the package to update on distribution points. It also doesn't cause clients to reevaluate policy for deployment of the package. After the ownership changes, make sure that the new site server can access the source files. It should have at least **Read** permissions to the source files of each package.

See also

- Fundamental concepts for content management
- The content library

Role-based Administration and Auditing Tool

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The Role-based Administration and Auditing Tool is one of the Configuration Manager tools. Use this tool for the following tasks:

- Model security roles with specific permissions
- Audit the security scopes and security roles that other users have

Requirements

- Run it on the same computer as the Configuration Manager console
- You have the **Full Administrator**, **Read-only Analyst**, or **Security Administrator** role
- Assign your account to the **All** security scope and all collections
- (*Optional*) To analyze report folder security, you must have SQL access
- (*Optional*) To analyze report drill-through, run this tool on the site system server with the reporting point role

Procedures

Model permissions for a new role

Use the following procedure to model permissions for a new role that you want to create:

1. Run **RBAViewer.exe**.
2. Select the base security roles you want to build on, or start from an empty permission set. Select the necessary permissions.
3. Click **Analyze** to see the user interface this custom role will see.

   > **NOTE**
   > To see whether there's an existing security role that meets your requirements, switch to the **Similarity** tab.

4. Click **Export** to save the role as an XML file. Then import it to the Configuration Manager console. For more information, see Create custom security roles.

Audit existing security scopes

Use the following procedure to audit all existing administrative users, collections, and security scopes in Configuration Manager:

1. Run **RBAViewer.exe**.
2. Select the **Audit RBA** button in the toolbar.
   a. To view the collection-limited relationships in a tree view, switch to the **Collection Summary** tab.
   b. To view objects assigned to a security role, switch to the **Scope Summary** tab.

Audit a specific user

Use the following procedure to audit the role-based administration configuration for a specific user:

1. Run **RBAViewer.exe**.
2. Select the **Run As** button in the toolbar.
3. Input the specific user name to check the permissions for that account.
4. The tool displays the security roles assigned to the user or the security group the user belongs to. It also displays the objects this user can see and the actions they can take in the console.

See also

- Fundamentals of role-based administration
- Configure role-based administration

Run Meter Summarization Tool

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The Run Meter Summarization Tool is one of the Configuration Manager tools. Use it to immediately trigger the maintenance tasks for software metering summarization on primary sites. By default, these tasks run as scheduled in **Site Maintenance** tasks, which start after 12:00 AM every day.

These tasks summarize the data in the **MeterData** SQL table, and write the summary results into the **FileUsageSummary** and **MonthlyUsageSummary** tables. Then you see the summarized result in software metering reports. Any Configuration Manager administrative user who can connect to the primary site database can use this tool to run summarization.

This tool runs the **File Usage Summary** and **Monthly Usage Summary** software metering data summarization tasks. It summarizes all existing meter data without the usual 12-hour waiting period. Run it on the SQL server that hosts the site database. If summarization is successful, the exit code is set to `0`. If there was an error, the exit code is `1`.

Usage

Command Line

```
runmetersumm [sms database name] <delay in hours for summarization <default=0>>
```

Options

Database name

The name of the site database on the SQL server.

Delay in hours for summarization

The tool summarizes the software metering usage generated before the delay. By default, this delay is zero.

Example

Summarize the software metering usage generated 12 hours ago

```
runmetersumm CCM_ABC <12>
```

See also

- Maintenance tasks
- Monitor app usage with software metering

Settings to manage high-risk deployments for Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

With Configuration Manager, you can configure deployment verification site settings. These settings warn administrators if they create a high-risk task sequence deployment. A high-risk deployment is:

- A deployment that's automatically installed
- Has the potential to cause unwanted results

For example, a task sequence with a purpose of **Required** that deploys an operating system is considered high-risk.

To reduce the risk of an unwanted high-risk deployment, you can configure size limits in these deployment verification settings:

- **Collection size limits**: When you create a deployment, hide collections that include more clients than your limit.
  - **Default size**: When you create a deployment, this setting hides collections by default that include more clients than this limit. You can still see these collections when creating the deployment, but they're hidden by default. The default value is **100**. To ignore this setting, enter a value of **0**.
  - **Maximum size**: When you create a deployment, this setting always hides collections with more clients than this limit. The default value is **0**, which ignores this setting. The **Maximum size** value must be greater than the **Default size** value.

    For example, you set **Default size** to 100 and the **Maximum size** to 1000. When you create a high-risk deployment, the **Select Collection** window only displays collections that include fewer than 100 clients. If you clear the setting to **Hide collections with a member count greater than the site's minimum size configuration**, the window displays collections that include fewer than 1000 clients.
- **Collections with site system servers**: When the target collection includes a computer with a site system role, block deployments or require verification before creating the deployment. When a deployment is blocked, select a different collection that meets the deployment verification criteria to continue creating the deployment.

> **NOTE**
> High-risk deployments are always limited to custom collections, collections that you create, and the built-in **Unknown Computers** collection. When you create a high-risk deployment, you can't select a built-in collection such as **All Systems**.

Configure deployment verification for a site

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, select **Sites**, and then select the primary site to configure.
2. Click **Properties** in the ribbon, and then switch to the **Deployment Verification** tab.
3. After setting configurations you want to use, click **OK** to save the configuration.

See also

Configure sites and hierarchies

Client installation methods in System Center Configuration Manager

2/12/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can use different methods to install the Configuration Manager client software. Use one method, or a combination of methods. This article describes each method, so you can learn which one works best for your organization.

Client push installation

Supported client platform: Windows

Advantages

- Can be used to install the client on a single computer, a collection of computers, or to the results from a query.
- Can be used to automatically install the client on all discovered computers.
- Automatically uses client installation properties defined on the **Client** tab in the **Client Push Installation Properties** dialog box.

Disadvantages

- Can cause high network traffic when pushing to large collections.
- Can only be used on computers that have been discovered by Configuration Manager.
- Can't be used to install clients in a workgroup.
- A client push installation account must be specified that has administrative rights to the intended client computer.
- Windows Firewall must be configured with exceptions on client computers.
- You can't cancel client push installation. Configuration Manager tries to install the client on all discovered resources. It retries any failures for up to seven days.

For more information, see How to install clients with client push.

Software update point-based installation

Supported client platform: Windows

Advantages

- Can use your existing software updates infrastructure to manage the client software.
- If Windows Server Update Services (WSUS) and group policy settings in Active Directory Domain Services are configured correctly, it can automatically install the client software on new computers.
- Doesn't require computers to be discovered before the client can be installed.
- Computers can read client installation properties that have been published to Active Directory Domain Services.

- If the client is removed, this method reinstalls it.
- Doesn't require you to configure and maintain an installation account for the intended client computer.

Disadvantages

- Requires a functioning software updates infrastructure as a prerequisite.
- Must use the same server for client installation and software updates. This server must reside in a primary site.
- To install new clients, you must configure a group policy object in Active Directory Domain Services with the client's active software update point and port.
- If the Active Directory schema isn't extended for Configuration Manager, you must use group policy settings to provision computers with client installation properties.

For more information, see How to install clients with software update-based installation.

Group policy installation

Supported client platform: Windows

Advantages

- Doesn't require computers to be discovered before the client can be installed.
- Can be used for new client installations or for upgrades.
- Computers can read client installation properties that have been published to Active Directory Domain Services.
- Doesn't require you to configure and maintain an installation account for the intended client computer.

Disadvantages

- If a large number of clients are being installed, it can cause high network traffic.
- If the Active Directory schema isn't extended for Configuration Manager, you must use group policy settings to add client installation properties to computers in your site.

For more information, see How to install clients with group policy.

Logon script installation

Supported client platform: Windows

Advantages

- Doesn't require computers to be discovered before the client can be installed.
- Supports using command-line properties for CCMSetup.

Disadvantages

- If a large number of clients are being installed over a short time period, it can cause high network traffic.
- If users don't frequently log on to the network, it can take a long time to install on all client computers.

For more information, see How to install clients with logon scripts.

Manual installation

Supported client platform: Windows, UNIX/Linux, Mac OS X

Advantages

- Doesn't require computers to be discovered before the client can be installed.
- Can be useful for testing purposes.
- Supports using command-line properties for CCMSetup.

Disadvantages

- No automation, therefore time consuming.

For more information about how to manually install the client on each of platform, see the following articles:

- How to deploy clients to Windows computers
- How to deploy clients to UNIX and Linux servers
- How to deploy clients to Macs

Microsoft Intune MDM installation

Supported client platforms: Windows 10

Advantages

- Doesn't require computers to be discovered before the client can be installed.
- Doesn't require you to configure and maintain an installation account for the intended client computer.
- Can use modern authentication with Azure Active Directory.
- Can install and assign computers on the internet.
- Can automate with Windows AutoPilot and Microsoft Intune for co-management.

Disadvantages

- Requires additional technologies outside of Configuration Manager.
- Requires the device have access to the internet, even if it is not internet-based.

For more information, see the following articles:

- How to install clients to Intune MDM-managed Windows devices
- Install and assign Configuration Manager Windows 10 clients using Azure AD for authentication

Prerequisites for deploying clients to Windows computers in Configuration Manager

8/28/2019 • 12 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Deploying Configuration Manager clients in your environment has the following external dependencies and dependencies within the product. Additionally, each client deployment method has its own dependencies that must be met for client installations to be successful.

For more information on the minimum hardware and OS requirements for the Configuration Manager client, see Supported configurations.

> **NOTE**
> The software version numbers shown in this article only list the minimum version numbers required.

Prerequisites for Windows clients

Use the following information to determine the prerequisites for when you install the Configuration Manager client on Windows devices.

Dependencies external to Configuration Manager

COMPONENT	DESCRIPTION
Windows Installer version 3.1.4000.2435	Required to support the use of Windows Installer update (.msp) files for packages and software updates.
Microsoft Background Intelligent Transfer Service (BITS) version 2.5	Required to allow throttled data transfers between the client computer and Configuration Manager site systems. BITS isn't automatically downloaded during client installation. When BITS is installed on computers, it typically requires a restart to complete the installation. Most operating systems include BITS. If they don't, install BITS before you install the Configuration Manager client.
Microsoft Task Scheduler	Enable this service on the client for the client installation to complete.
SHA-2 code signing support	Starting in version 1906, clients require support for the SHA-2 code signing algorithm. For more information, see SHA-2 code signing support.

SHA-2 code signing support

Due to weaknesses in the SHA-1 algorithm and to align to industry standards, Microsoft now only signs Configuration Manager binaries using the more secure SHA-2 algorithm. The following Windows OS versions require an update for SHA-2 code signing support:

- Windows 7 SP1
- Windows Server 2008 R2 SP1

- Windows Server 2008 SP2

For more information, see 2019 SHA-2 code signing support requirement for Windows and WSUS.

If you don't update these OS versions, you can't install the Configuration Manager client version 1906. This behavior applies to either a new client install or updating it from a previous version.

If you need to manage a client on a version of Windows that's not updated, or older than the versions listed above, use the Configuration Manager extended interoperability client (EIC) version 1902. For more information, see Extended interoperability client.

> **TIP**
>
> If you don't use automatic client update, and update clients with another mechanism, make sure to update the version of ccmsetup. An older version of ccmsetup may not properly validate the new SHA-2 code signing certificate on the version 1906 client binaries. For example, if you copy ccmsetup.exe to a file share, or use ccmsetup.msi with group policy.
>
> The following client update mechanisms shouldn't be affected:
>
> - Client push installation: It uses the client package from the site
> - Software update-based installation: The site update republishes to WSUS
> - Intune MDM-managed Windows devices: The supported version for this mechanism already supports SHA-2 code signing, but it's still important to use the latest ccmsetup.msi

Dependencies external to Configuration Manager and automatically downloaded during installation

The Configuration Manager client has external dependencies. These dependencies depend on the OS version and the installed software on the client computer.

If the client requires these dependencies to complete the installation, it automatically installs them.

COMPONENT	DESCRIPTION
Windows Update Agent version 7.0.6000.363	Required by Windows to support update detection and deployment.
Microsoft Core XML Services (MSXML) version 6.20.5002 or later	Required to support the processing of XML documents in Windows.
Microsoft Remote Differential Compression (RDC)	Required to optimize data transmission over the network.
Microsoft Visual C++ 2013 Redistributable version 12.0.21005.1	Required to support client operations. When you install this update on client computers, it might require a restart to complete the installation.
Microsoft Visual C++ 2005 Redistributable version 8.0.50727.42	For version 1606 and earlier, required to support Microsoft SQL Server Compact operations.
Windows Imaging APIs 6.0.6001.18000	Required to allow Configuration Manager to manage Windows image (.wim) files.
Microsoft Policy Platform 1.2.3514.0	Required to allow clients to evaluate compliance settings.
Microsoft .NET Framework version 4.5.2	Required to support client operations. Automatically installed on the client computer if it doesn't have Microsoft .NET Framework version 4.5 or later installed. For more information, see Additional details about Microsoft .NET Framework version 4.5.2.

COMPONENT	DESCRIPTION
Microsoft SQL Server Compact 4.0 SP1 components	Required to store information related to client operations.

> **IMPORTANT**
>
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features
>
> If you're still using the application catalog website user experience, the client requires Microsoft Silverlight 5.1.41212.0. Starting in Configuration Manager 1802, the client doesn't automatically install Silverlight. The primary functionality of the application catalog is now included in Software Center.

Additional details about Microsoft .NET Framework version 4.5.2

> **NOTE**
>
> .NET 4.0, 4.5, and 4.5.1 are no longer supported. For more information, see Microsoft .NET Framework Support Lifecycle Policy FAQ.

Microsoft .NET Framework version 4.5.2 may require a restart to complete the installation. The user sees a **Restart required** notification in the system tray. The following common scenarios require client computers to restart:

- .NET applications or services are running on the computer.
- One or more software updates required for .NET installation are missing.
- The computer is pending a restart from prior installation of .NET framework software updates.

After .NET Framework 4.5.2 is installed, it may require additional updates. These later updates may require additional computer restarts.

Configuration Manager dependencies

For more information, see Determine the site system roles for clients.

COMPONENT	DESCRIPTION
Management point	To deploy the Configuration Manager client, you don't require a management point. Clients require a management point to transfer information with the site. Without a management point, you can't manage client computers.
Distribution point	The distribution point is an optional, but recommended site system role for client deployment and management. All distribution points host the client source files. Clients find the nearest distribution point from which to download the source files during client deployment or update. If the site doesn't have a distribution point, computers download the client source files from their management point.

COMPONENT	DESCRIPTION
Fallback status point	The fallback status point is an optional, but recommended site system role for client deployment. The fallback status point tracks client deployment and enables computers in the Configuration Manager site to send state messages when they can't communicate with a management point.
Reporting services point	The reporting services point is an optional, but recommended site system role. It displays reports related to client deployment and management. For more information, see Reporting in Configuration Manager.

Installation method dependencies

The following prerequisites are specific to the various methods of client installation.

Client push installation

- The site uses client push installation accounts to connect to computers to install the client. Specify these accounts on the **Accounts** tab of the Client Push Installation Properties. The account must be a member of the local administrators group on the destination computer.

  If you don't specify a client push installation account, the site server uses its computer account.

- The site needs to discover the computer on which you're installing the client. At least one Configuration Manager discovery method is needed.

- The computer has an ADMIN$ share.

- To automatically push the Configuration Manager client to discovered resources, select the option to **Enable client push installation to assigned resources** in the Client Push Installation Properties.

- The client computer needs to communicate with a distribution point or a management point to download the source files.

- Starting in version 1806, when you require Kerberos mutual authentication, clients must be in a trusted Active Directory forest. Kerberos in Windows relies upon Active Directory for mutual authentication.

To use client push, you need the following security permissions:

- To configure the client push installation account: **Modify** and **Read** permission for the **Site** object.

- To use client push to install the client to collections, devices and queries: **Modify Resource** and **Read** permission for the **Collection** object.

The **Infrastructure Administrator** default security role includes the required permissions to manage client push installations.

Software update point-based installation

- If you haven't extended the Active Directory schema, or you're installing clients from another forest, use group policy to provision installation parameters for CCMSetup.exe. For more information, see How to provision client installation properties.

- Publish the Configuration Manager client to the software update point.

- To download the source files, the client computer needs to communicate with a distribution point or a management point.

For the security permissions required to manage Configuration Manager software updates, see Prerequisites for software updates.

Group policy-based installation

- If you haven't extended the Active Directory schema, or you're installing clients from another forest, use group policy to provision installation parameters for CCMSetup.exe. For more information, see How to provision client installation properties.
- To download the source files, the client computer needs to communicate with a distribution point or a management point.

Logon script-based installation

To download the source files, the client computer needs to communicate with a distribution point or a management point. Unless you specified CCMSetup.exe with the following command-line parameter: `ccmsetup /source`

Manual installation

To download the source files, the client computer needs to communicate with a distribution point or a management point. Unless you specified CCMSetup.exe with the following command-line parameter: `ccmsetup /source`

Microsoft Intune MDM installation

> **IMPORTANT**
> Hybrid mobile device management is a deprecated feature.

- Requires a Microsoft Intune subscription and appropriate licenses.
- Requires the device has internet access, even if it isn't internet-based.
- Depending upon the use case, you may also require one or both of the following technologies:
  - Azure Active Directory
  - Cloud management gateway

Workgroup computer installation

To access resources in the Configuration Manager site server's domain, configure a network access account for the site.

For more information about how to configure the network access account, see the Fundamental concepts for content management.

Software distribution-based installation (for upgrades only)

- If you haven't extended the Active Directory schema, or you're installing clients from another forest, use group policy to provision installation parameters for CCMSetup.exe. For more information, see How to provision client installation properties.
- To download the source files, the client computer needs to communicate with a distribution point or a management point.

For the security permissions required to upgrade the Configuration Manager client using application management, see Security and privacy for application management.

Automatic client upgrades

You must be a member of the **Full Administrator** security role to configure automatic client upgrades.

Firewall requirements

If there's a firewall between the site system servers and the computers onto which you want to install the Configuration Manager client, see Windows Firewall and port settings for clients.

Prerequisites for mobile device clients

When you install the Configuration Manager client on mobile devices and enroll them, use this information to determine the prerequisites.

Dependencies external to Configuration Manager

- A Microsoft enterprise certification authority (CA) with certificate templates to deploy and manage the certificates required for mobile devices.

  The issuing CA must automatically approve certificate requests from the mobile device users during the enrollment process.

  For more information about the certificate requirements, see Security and privacy for certificate profiles.

- A security group that contains the users that can enroll their mobile devices.

  This security group is used to configure the certificate template that is used during mobile device enrollment.

- Optional but recommended: a DNS alias (CNAME record) named **ConfigMgrEnroll**. Configure this alias for the server name of the enrollment proxy point.

  This DNS alias is required to support automatic discovery for the enrollment service. If you don't configure this DNS record, users must manually specify the name of the enrollment proxy point as part of the enrollment process.

- Site system role dependencies for the computers that run the enrollment point and the enrollment proxy point site system roles.

  For more information, see Supported operating systems for site system servers.

Configuration Manager dependencies

For more information, see Determine the site system roles for clients.

- Management point that's configured for HTTPS client connections and enabled for mobile devices

  A management point is always required to install the Configuration Manager client on mobile devices. In addition to the configuration requirements of HTTPS and enabled for mobile devices, the management point must be configured with an internet FQDN and accept client connections from the internet.

- Enrollment point and enrollment proxy point

  An enrollment proxy point manages enrollment requests from mobile devices and the enrollment point completes the enrollment process. The enrollment point must be in the same Active Directory forest as the site server, but the enrollment proxy point can be in another forest.

- Client settings for mobile device enrollment

  Configure client settings to allow users to enroll mobile devices and configure at least one enrollment profile.

- Reporting services point

  The reporting services point is an optional, but recommended site system role that can display reports related to mobile device enrollment and client management.

  For more information, see Reporting in Configuration Manager.

- To configure enrollment for mobile devices, you must have the following security permissions:
  - To add, modify, and delete the enrollment site system roles: **Modify** permission for the **Site** object.
  - To configure client settings for enrollment: Default client settings require **Modify** permission for the

Site object, and custom client settings require **Client agent** permissions.

The **Full Administrator** default security role includes the required permissions to configure the enrollment site system roles.

- To manage enrolled mobile devices, you must have the following security permissions:
  - To wipe or retire a mobile device: **Delete resource** for the **Collection** object.
  - To cancel a wipe or retire command: **Delete resource** for the **Collection** object.
  - To allow and block mobile devices: **Modify resource** for the **Collection** object.
  - To remote lock, or reset the passcode on a mobile device: **Modify** resource for the **Collection** object.

  The **Operations Administrator** default security role includes the required permissions to manage mobile devices.

  For more information about how to configure security permissions, see Fundamentals of role-based administration and Configure role-based administration.

Firewall requirements

Intervening network devices such as routers and firewalls, and Windows Firewall if applicable, must allow the traffic associated with mobile device enrollment:

- Between mobile devices and the enrollment proxy point: HTTPS (by default, TCP 443)
- Between the enrollment proxy point and the enrollment point: HTTPS (by default, TCP 443)

If you use a proxy web server, it must be configured for SSL tunneling. SSL bridging isn't supported for mobile devices.

Windows Firewall and port settings for clients in System Center Configuration Manager

2/12/2019 • 8 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Client computers in System Center Configuration Manager that run Windows Firewall often require you to configure exceptions to allow communication with their site. The exceptions that you must configure depend on the management features that you use with the Configuration Manager client.

Use the following sections to identify these management features and for more information about how to configure Windows Firewall for these exceptions.

Modifying the Ports and Programs Permitted by Windows Firewall

Use the following procedure to modify the ports and programs on Windows Firewall for the Configuration Manager client.

To modify the ports and programs permitted by Windows Firewall

1. On the computer that runs Windows Firewall, open Control Panel.
2. Right-click **Windows Firewall**, and then click **Open**.
3. Configure any required exceptions and any custom programs and ports that you require.

Programs and Ports that Configuration Manager Requires

The following Configuration Manager features require exceptions on the Windows Firewall:

Queries

If you run the Configuration Manager console on a computer that runs Windows Firewall, queries fail the first time that they are run and the operating system displays a dialog box asking if you want to unblock statview.exe. If you unblock statview.exe, future queries will run without errors. You can also manually add Statview.exe to the list of programs and services on the **Exceptions** tab of the Windows Firewall before you run a query.

Client Push Installation

To use client push to install the Configuration Manager client, add the following as exceptions to the Windows Firewall:

- Outbound and inbound: **File and Printer Sharing**
- Inbound: **Windows Management Instrumentation (WMI)**

Client Installation by Using Group Policy

To use Group Policy to install the Configuration Manager client, add **File and Printer Sharing** as an exception to the Windows Firewall.

Client Requests

For client computers to communicate with Configuration Manager site systems, add the following as exceptions to the Windows Firewall:

Outbound: TCP Port **80** (for HTTP communication)

Outbound: TCP Port **443** (for HTTPS communication)

> **IMPORTANT**
> These are default port numbers that can be changed in Configuration Manager. For more information, see How to How to configure client communication ports in System Center Configuration Manager. If these ports have been changed from the default values, you must also configure matching exceptions on the Windows Firewall.

Client Notification

For the management point to notify client computers about an action that it must take when an administrative user selects a client action in the Configuration Manager console, such as download computer policy or initiate a malware scan, add the following as an exception to the Windows Firewall:

Outbound: TCP Port **10123**

If this communication does not succeed, Configuration Manager automatically falls back to using the existing client-to-management point communication port of HTTP, or HTTPS:

Outbound: TCP Port **80** (for HTTP communication)

Outbound: TCP Port **443** (for HTTPS communication)

> **IMPORTANT**
> These are default port numbers that can be changed in Configuration Manager. For more information, see How to configure client communication ports in System Center Configuration Manager. If these ports have been changed from the default values, you must also configure matching exceptions on the Windows Firewall.

Remote Control

To use Configuration Manager remote control, allow the following port:

- Inbound: TCP Port **2701**

Remote Assistance and Remote Desktop

To initiate Remote Assistance from the Configuration Manager console, add the custom program **Helpsvc.exe** and the inbound custom port TCP **135** to the list of permitted programs and services in Windows Firewall on the client computer. You must also permit **Remote Assistance** and **Remote Desktop**. If you initiate Remote Assistance from the client computer, Windows Firewall automatically configures and permits **Remote Assistance** and **Remote Desktop**.

Wake-Up Proxy

If you enable the wake-up proxy client setting, a new service named ConfigMgr Wake-up Proxy uses a peer-to-peer protocol to check whether other computers are awake on the subnet and to wake them up if necessary. This communication uses the following ports:

Outbound: UDP Port **25536**

Outbound: UDP Port **9**

These are the default port numbers that can be changed in Configuration Manager by using the **Power Management** clients settings of **Wake-up proxy port number (UDP)** and **Wake On LAN port number (UDP)**. If you specify the **Power Management**: **Windows Firewall exception for wake-up proxy** client setting, these ports are automatically configured in Windows Firewall for clients. However, if clients run a different firewall, you must manually configure the exceptions for these port numbers.

In addition to these ports, wake-up proxy also uses Internet Control Message Protocol (ICMP) echo request

messages from one client computer to another client computer. This communication is used to confirm whether the other client computer is awake on the network. ICMP is sometimes referred to as TCP/IP ping commands.

For more information about wake-up proxy, see Plan how to wake up clients in System Center Configuration Manager.

Windows Event Viewer, Windows Performance Monitor, and Windows Diagnostics

To access Windows Event Viewer, Windows Performance Monitor, and Windows Diagnostics from the Configuration Manager console, enable **File and Printer Sharing** as an exception on the Windows Firewall.

Ports Used During Configuration Manager Client Deployment

The following tables list the ports that are used during the client installation process.

> **IMPORTANT**
> If there is a firewall between the site system servers and the client computer, confirm whether the firewall permits traffic for the ports that are required for the client installation method that you choose. For example, firewalls often prevent client push installation from succeeding because they block Server Message Block (SMB) and Remote Procedure Calls (RPC). In this scenario, use a different client installation method, such as manual installation (running CCMSetup.exe) or Group Policy-based client installation. These alternative client installation methods do not require SMB or RPC.

For information about how to configure Windows Firewall on the client computer, see Modifying the Ports and Programs Permitted by Windows Firewall.

Ports that are used for all installation methods

DESCRIPTION	UDP	TCP
Hypertext Transfer Protocol (HTTP) from the client computer to a fallback status point, when a fallback status point is assigned to the client.	--	80 (See note 1, **Alternate Port Available**)

Ports that are used with client push installation

In addition to the ports listed in the following table, client push installation also uses Internet Control Message Protocol (ICMP) echo request messages from the site server to the client computer to confirm whether the client computer is available on the network. ICMP is sometimes referred to as TCP/IP ping commands. ICMP does not have a UDP or TCP protocol number, and so it is not listed in the following table. However, any intervening network devices, such as firewalls, must permit ICMP traffic for client push installation to succeed.

DESCRIPTION	UDP	TCP
Server Message Block (SMB) between the site server and client computer.	--	445
RPC endpoint mapper between the site server and the client computer.	135	135
RPC dynamic ports between the site server and the client computer.	--	DYNAMIC

DESCRIPTION	UDP	TCP
Hypertext Transfer Protocol (HTTP) from the client computer to a management point when the connection is over HTTP.	--	80 (See note 1, **Alternate Port Available**)
Secure Hypertext Transfer Protocol (HTTPS) from the client computer to a management point when the connection is over HTTPS.	--	443 (See note 1, **Alternate Port Available**)

Ports that are used with software update point-based installation

DESCRIPTION	UDP	TCP
Hypertext Transfer Protocol (HTTP) from the client computer to the software update point.	--	80 or 8530 (See note 2, **Windows Server Update Services**)
Secure Hypertext Transfer Protocol (HTTPS) from the client computer to the software update point.	--	443 or 8531 (See note 2, **Windows Server Update Services**)
Server Message Block (SMB) between the source server and the client computer when you specify the CCMSetup command-line property **/source:<Path>**.	--	445

Ports that are used with Group Policy-based installation

DESCRIPTION	UDP	TCP
Hypertext Transfer Protocol (HTTP) from the client computer to a management point when the connection is over HTTP.	--	80 (See note 1, **Alternate Port Available**)
Secure Hypertext Transfer Protocol (HTTPS) from the client computer to a management point when the connection is over HTTPS.	--	443 (See note 1, **Alternate Port Available**)
Server Message Block (SMB) between the source server and the client computer when you specify the CCMSetup command-line property **/source:<Path>**.	--	445

Ports that are used with manual installation and logon script-based installation

DESCRIPTION	UDP	TCP
Server Message Block (SMB) between the client computer and a network share from which you run CCMSetup.exe. When you install Configuration Manager, the client installation source files are copied and automatically shared from the *<InstallationPath>*\Client folder on management points. However, you can copy these files and create a new share on any computer on the network. Alternatively, you can eliminate this network traffic by running CCMSetup.exe locally, for example, by using removable media.	--	445
Hypertext Transfer Protocol (HTTP) from the client computer to a management point when the connection is over HTTP, and you do not specify the CCMSetup command-line property **/source:<Path>**.	--	80 (See note 1, **Alternate Port Available**)
Secure Hypertext Transfer Protocol (HTTPS) from the client computer to a management point when the connection is over HTTPS, and you do not specify the CCMSetup command-line property **/source:<Path>**.	--	443 (See note 1, **Alternate Port Available**)
Server Message Block (SMB) between the source server and the client computer when you specify the CCMSetup command-line property **/source:<Path>**.	--	445

Ports that are used with software distribution-based installation

DESCRIPTION	UDP	TCP
Server Message Block (SMB) between the distribution point and the client computer.	--	445
Hypertext Transfer Protocol (HTTP) from the client to a distribution point when the connection is over HTTP.	--	80 (See note 1, **Alternate Port Available**)
Secure Hypertext Transfer Protocol (HTTPS) from the client to a distribution point when the connection is over HTTPS.	--	443 (See note 1, **Alternate Port Available**)

Notes

1 Alternate Port Available In Configuration Manager, you can define an alternate port for this value. If a custom port has been defined, substitute that custom port when you define the IP filter information for IPsec policies or for configuring firewalls.

2 Windows Server Update Services You can install Windows Server Update Service (WSUS) either on the default Web site (port 80) or a custom Web site (port 8530).

After installation, you can change the port. You do not have to use the same port number throughout the site hierarchy.

If the HTTP port is 80, the HTTPS port must be 443.

If the HTTP port is anything else, the HTTPS port must be 1 higher. For example, 8530 and 8531.

Determine the site system roles for Configuration Manager clients

7/26/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article can help you determine the site system roles that you need to deploy Configuration Manager clients.

For more information about where to install these roles in the hierarchy, see Design a hierarchy of sites.

For more information about how to install and configure these roles, see Install site system roles.

Management point

By default, all Windows client computers use a distribution point to install the Configuration Manager client. They can fall back to a management point when a distribution point is unavailable. However, you can install Windows clients on computers from an alternative source when you use the CCMSetup command-line property `/source:<Path>`. For example, you might do this action if you install clients on the internet. Another scenario is when you want to avoid sending network packets between the computer and the management point during client installation. This scenario is because a firewall blocks the required ports or because you have a low-bandwidth connection. However, all clients must communicate with a management point to assign to a site and to be managed by Configuration Manager.

For more information about client command-line properties, see About client installation properties.

When you install more than one management point in the hierarchy, clients automatically connect to one point based on their forest membership and network location. You can't install more than one management point in a secondary site.

Mac computer clients and mobile device clients that you enroll with Configuration Manager always require a management point for client installation. This management point must be in a primary site, must be configured to support mobile devices, and must accept client connections from the Internet. These clients can't use management points in secondary sites or connect to management points in other primary sites.

Distribution point

You don't need a distribution point to install Configuration Manager clients on Windows computers. By default, Configuration Manager uses a distribution point to install the client source files on Windows computers. It can fall back to downloading these files from a management point. Distribution points aren't used to install mobile device clients that are enrolled by Configuration Manager, but are used if you install the mobile device legacy client. If you install the Configuration Manager client as part of an OS deployment, the OS image is stored and retrieved from a distribution point.

Although you might not need distribution points to install most Configuration Manager clients, you'll need them to install software such as applications and software updates on the clients.

Fallback status point

You can use a fallback status point to monitor client deployment for Windows computers. You can also identify the Windows computer clients that are unmanaged because they can't communicate with a management point.

The following client types don't use a fallback status point:

- Mac computers
- Mobile devices that are enrolled by Configuration Manager
- Mobile devices that are managed by using the Exchange Server connector

A fallback status point isn't required to monitor client activity and client health.

The fallback status point always communicates with clients over HTTP, which uses unauthenticated connections and sends data in clear text. This behavior makes the fallback status point vulnerable to attack, particularly when it's used with internet-based client management. To help reduce the attack surface, always dedicate a server to running the fallback status point. Don't install other site system roles on the same server in a production environment.

Install a fallback status point if all the following conditions apply:

- You want client communication errors from Windows computers to be sent to the site, even if these client computers can't communicate with a management point.
- You want to use the Configuration Manager client deployment reports, which display the data that's sent by the fallback status point.
- You have a dedicated server for this site system role and have additional security measures to help protect the server from attack.
- The benefits of using a fallback status point outweigh any security risks associated with unauthenticated connections and clear text transfers over HTTP traffic.

Don't install a fallback status point if the security risks of running a website with unauthenticated connections and clear text transfers outweigh the benefits of identifying client communication problems.

Reporting services point

Configuration Manager provides many reports to help you monitor the installation, assignment, and management of clients in the Configuration Manager console. Some of the client deployment reports require that clients are assigned to a fallback status point.

The reports aren't needed to deploy clients. You can see some deployment information in the Configuration Manager console or use the client log files for detailed information. However, the client reports provide valuable information to help monitor and troubleshoot client deployment.

Enrollment point and enrollment proxy point

Configuration Manager requires the enrollment point and the enrollment proxy point to enroll mobile devices and to enroll certificates for Mac computers. You don't need these site system roles in the following situations:

- You plan to manage mobile devices by using the Exchange Server connector
- You install the mobile device legacy client, for example, for Windows CE
- You request and install the client certificate on Mac computers independently from Configuration Manager

Application catalog

IMPORTANT

The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.

For more information, see the following articles:

- Configure Software Center
- Removed and deprecated features

Cloud management gateway connector point

You need a cloud management gateway connector point if you're setting up a cloud management gateway to manage clients on the internet.

Security and privacy for Configuration Manager clients

7/9/2019 • 23 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article describes security and privacy information for Configuration Manager clients. It also includes information for mobile devices that are managed by the Exchange Server connector.

Security best practices for clients

The Configuration Manager site accepts data from devices that run the Configuration Manager client. This behavior introduces the risk that the clients could attack the site. For example, they could send malformed inventory, or attempt to overload the site systems. Deploy the Configuration Manager client only to devices that you trust. In addition, use the following security best practices to help protect the site from rogue or compromised devices:

Use public key infrastructure (PKI) certificates for client communications with site systems that run IIS

- As a site property, configure **Site system settings** for **HTTPS only**.
- Install clients with the `UsePKICert` CCMSetup property.
- Use a certificate revocation list (CRL) and make sure that clients and communicating servers can always access it.

Mobile device clients and some internet-based clients require these certificates. Microsoft recommends these certificates for all client connections on the intranet.

For more information about the PKI certificate requirements and how they're used to help protect Configuration Manager, see PKI certificate requirements.

Automatically approve client computers from trusted domains and manually check and approve other computers

When you can't use PKI authentication, approval identifies a computer that you trust to be managed by Configuration Manager. The hierarchy has the following options to configure client approval:

- Manual
- Automatic for computers in trusted domains
- Automatic for all computers

The most secure approval method is to automatically approve clients that are members of trusted domains. Then manually check and approve all other computers. Automatically approving all clients isn't recommended, unless you have other access controls to prevent untrustworthy computers from accessing your network.

For more information about how to manually approve computers, see Manage clients from the devices node.

Don't rely on blocking to prevent clients from accessing the Configuration Manager hierarchy

Blocked clients are rejected by the Configuration Manager infrastructure. If clients are blocked, they can't communicate with site systems to download policy, upload inventory data, or send state or status messages.

Blocking is designed for the following scenarios:

- To block lost or compromised boot media when you deploy an OS to clients

- When all site systems accept HTTPS client connections

When site systems accept HTTP client connections, don't rely on blocking to protect the Configuration Manager hierarchy from untrusted computers. In this scenario, a blocked client could rejoin the site with a new self-signed certificate and hardware ID.

Certificate revocation is the primary line of defense against potentially compromised certificates. A certificate revocation list (CRL) is only available from a supported public key infrastructure (PKI). Blocking clients in Configuration Manager offers a second line of defense to protect your hierarchy.

For more information, see Determine whether to block clients.

Use the most secure client installation methods that are practical for your environment

- For domain computers, Group Policy client installation and software update-based client installation methods are more secure than client push installation.
- If you apply access controls and change controls, use imaging and manual installation methods.
- In version 1806 or later, use Kerberos mutual authentication with client push installation.

Of all the client installation methods, client push installation is the least secure because of the many dependencies it has. These dependencies include local administrative permissions, the Admin$ share, and firewall exceptions. The number and type of these dependencies increase your attack surface.

Starting in version 1806, when using client push, the site can require Kerberos mutual authentication by not allowing fallback to NTLM before establishing the connection. This enhancement helps to secure the communication between the server and the client. For more information, see How to install clients with client push.

For more information about the different client installation methods, see Client installation methods.

Wherever possible, select a client installation method that requires the least security permissions in Configuration Manager. Restrict the administrative users that are assigned security roles with permissions that can be used for purposes other than client deployment. For example, configuring automatic client upgrade requires the **Full Administrator** security role, which grants an administrative user all security permissions.

For more information about the dependencies and security permissions required for each client installation method, see "Installation method dependencies" in Prerequisites for computer clients.

If you must use client push installation, take additional steps to secure the Client Push Installation Account

This account must be a member of the local **Administrators** group on each computer that installs the Configuration Manager client. Never add the Client Push Installation Account to the **Domain Admins** group. Instead, create a global group, and then add that global group to the local **Administrators** group on your clients. Create a group policy object to add a Restricted Group setting to add the Client Push Installation Account to the local **Administrators** group.

For additional security, create multiple Client Push Installation Accounts, each with administrative access to a limited number of computers. If one account is compromised, only the client computers to which that account has access are compromised.

Remove certificates before imaging clients

When you deploy clients by using OS images, always remove certificates before capturing the image. These certificates include PKI certificates for client authentication, and self-signed certificates. If you don't remove these certificates, clients might impersonate each other. You can't verify the data for each client.

For more information, see Create a task sequence to capture an operating system.

Ensure that the Configuration Manager computer clients get an authorized copy of these certificates

The Configuration Manager trusted root key certificate

When both of the following statements are true, clients rely on the Configuration Manager trusted root key to authenticate valid management points:

- You haven't extended the Active Directory schema for Configuration Manager
- Clients don't use PKI certificates when they communicate with management points

In this scenario, clients have no way to verify that the management point is trusted for the hierarchy unless they use the trusted root key. Without the trusted root key, a skilled attacker could direct clients to a rogue management point.

When clients can't download the Configuration Manager trusted root key from the Global Catalog or by using PKI certificates, pre-provision the clients with the trusted root key. This action makes sure that they can't be directed to a rogue management point. For more information, see Planning for the trusted root key.

The site server signing certificate

Clients use this certificate to verify that the site server signed the policy downloaded from a management point. This certificate is self-signed by the site server and published to Active Directory Domain Services.

When clients can't download the site server signing certificate from the Global Catalog, by default they download it from the management point. If the management point is exposed to an untrusted network like the internet, manually install the site server signing certificate on clients. This action makes sure that they can't download tampered client policies from a compromised management point.

To manually install the site server signing certificate, use the CCMSetup client.msi property **SMSSIGNCERT**. For more information, see About client installation properties.

Don't use automatic site assignment if the client downloads the trusted root key from the first management point it contacts

To avoid the risk of a new client downloading the trusted root key from a rogue management point, only use automatic site assignment in the following scenarios:

- The client can access Configuration Manager site information that's published to Active Directory Domain Services.
- You pre-provision the client with the trusted root key.
- You use PKI certificates from an enterprise certification authority to establish trust between the client and the management point.

For more information about the trusted root key, see Planning for the trusted root key.

Install client computers with the CCMSetup Client.msi option SMSDIRECTORYLOOKUP=NoWINS

The most secure service location method for clients to find sites and management points is to use Active Directory Domain Services. Sometimes this method isn't possible for some environments. For example, because you can't extend the Active Directory schema for Configuration Manager, or because clients are in an untrusted forest or a workgroup. If this method isn't possible, use DNS publishing as an alternative service location method. If both these methods fail, and when the management point isn't configured for HTTPS client connections, clients can fall back to using WINS.

Publishing to WINS is less secure than the other publishing methods. Configure client computers to not fall back to using WINS by specifying **SMSDIRECTORYLOOKUP=NoWINS**. If you must use WINS for service location, use **SMSDIRECTORYLOOKUP=WINSSECURE**. This setting is the default. It uses the Configuration Manager trusted root key to validate the self-signed certificate of the management point.

> **NOTE**
>
> When you configure the client for **SMSDIRECTORYLOOKUP=WINSSECURE** and it finds a management point from WINS, the client checks its copy of the Configuration Manager trusted root key that's in WMI.
>
> If the signature on the management point certificate matches the client's copy of the trusted root key, the certificate is validated. After validating the certificate, the client starts communicates with the management point that it found by using WINS.
>
> If the signature on the management point certificate doesn't match the client's copy of the trusted root key, the certificate isn't valid. In this scenario, the client doesn't communicate with the management point that it found by using WINS.

Make sure that maintenance windows are large enough to deploy critical software updates

Maintenance windows for device collections restrict the times that Configuration Manager can install software on these devices. If you configure the maintenance window to be too small, the client may not install critical software updates. This behavior leaves the client vulnerable to any attack that the software update mitigates.

Take additional security precautions to reduce the attack surface on Windows embedded devices with write filters

When you enable write filters on Windows Embedded devices, any software installations or changes are only made to the overlay. These changes don't persist after the device restarts. If you use Configuration Manager to disable the write filters, during this period the embedded device is vulnerable to changes to all volumes. These volumes include shared folders.

Configuration Manager locks the computer during this period so that only local administrators can sign in. Whenever possible, take additional security precautions to help protect the computer. For example, enable additional restrictions on the firewall.

If you use maintenance windows to persist changes, plan these windows carefully. Minimize the time that write filters are disabled, but make them long enough to allow software installations and restarts to complete.

Use the latest client version with software update-based client installation

If you use software update-based client installation, and install a later version of the client on the site, update the published software update. Then clients receive the latest version from the software update point.

When you update the site, the software update for client deployment that's published to the software update point isn't automatically updated. Republish the Configuration Manager client to the software update point and update the version number.

For more information, see How to install Configuration Manager clients by using software update-based installation.

Only suspend BitLocker PIN entry on trusted and restricted-access devices

Only configure the client setting to **Suspend BitLocker PIN entry on restart** to **Always** for computers that you trust and that have restricted physical access.

When you set this client setting to **Always**, Configuration Manager can complete the installation of software. This behavior helps install critical software updates and resume services. If an attacker intercepts the restart process, they could take control of the computer. Use this setting only when you trust the computer, and when physical access to the computer is restricted. For example, this setting might be appropriate for servers in a data center.

For more information on this client setting, see About client settings.

Don't bypass PowerShell execution policy

If you configure the Configuration Manager client setting for **PowerShell execution policy** to **Bypass**, then Windows allows unsigned PowerShell scripts to run. This behavior could allow malware to run on client computers. When your organization requires this option, use a custom client setting. Assign it to only the client

computers that must run unsigned PowerShell scripts.

For more information on this client setting, see About client settings.

Security best practices for mobile devices

Install the enrollment proxy point in a perimeter network and the enrollment point in the intranet

For internet-based mobile devices that you enroll with Configuration Manager, install the enrollment proxy point in a perimeter network and the enrollment point in the intranet. This role separation helps to protect the enrollment point from attack. If an attacker compromises the enrollment point, they could obtain certificates for authentication. They can also steal the credentials of users who enroll their mobile devices.

Configure the password settings to help protect mobile devices from unauthorized access

For mobile devices that are enrolled by Configuration Manager: Use a mobile device configuration item to configure the password complexity as the PIN. Specify at least the default minimum password length.

For mobile devices that don't have the Configuration Manager client installed but are managed by the Exchange Server connector: Configure the **Password Settings** for the Exchange Server connector such that the password complexity is the PIN. Specify at least the default minimum password length.

Only allow applications to run that are signed by companies that you trust

Help prevent tampering of inventory information and status information by allowing applications to run only when they're signed by companies that you trust. Don't allow devices to install unsigned files.

For mobile devices that are enrolled by Configuration Manager: Use a mobile device configuration item to configure the security setting **Unsigned applications** as **Prohibited**. Configure **Unsigned file installations** to be a trusted source.

For mobile devices that don't have the Configuration Manager client installed but are managed by the Exchange Server connector: Configure the **Application Settings** for the Exchange Server connector such that **Unsigned file installation** and **Unsigned applications** are **Prohibited**.

Lock mobile devices when not in use

Help prevent elevation of privilege attacks by locking the mobile device when it isn't used.

For mobile devices that are enrolled by Configuration Manager: Use a mobile device configuration item to configure the password setting **Idle time in minutes before mobile device is locked**.

For mobile devices that don't have the Configuration Manager client installed but are managed by the Exchange Server connector: Configure the **Password Settings** for the Exchange Server connector to set the **Idle time in minutes before mobile device is locked**.

Restrict the users who can enroll their mobile devices

Help prevent elevation of privileges by restricting the users who can enroll their mobile devices. Use a custom client setting rather than default client settings to allow only authorized users to enroll their mobile devices.

User device affinity guidance for mobile devices

Don't deploy applications to users who have mobile devices enrolled by Configuration Manager or Microsoft Intune in the following scenarios:

- The mobile device is used by more than one person.
- The device is enrolled by an administrator on behalf of a user.
- The device is transferred to another person without retiring and then re-enrolling the device.

Device enrollment creates a user device affinity relationship. This relationship maps the user who performs

enrollment to the mobile device. If another user uses the mobile device, they can run the applications deployed to the original user, which might result in an elevation of privileges. Similarly, if an administrator enrolls the mobile device for a user, applications deployed to the user aren't installed on the mobile device. Instead, applications deployed to the administrator might be installed.

Unlike user device affinity for Windows computers, you can't manually define the user device affinity information for mobile devices enrolled by Microsoft Intune.

If you transfer ownership of a mobile device that's enrolled by Intune, first retire the mobile device from Intune. This action removes the user device affinity relationship. Then ask the current user to enroll the device again.

Make sure that users enroll their own mobile devices for Microsoft Intune

A user device affinity relationship is created during enrollment. This action maps the user who performs enrollment to the mobile device. If an administrator enrolls the mobile device for a user, applications deployed to the user aren't installed on the mobile device. Instead, applications deployed to the administrator might be installed.

Protect the connection between the Configuration Manager site server and the Exchange Server

If the Exchange Server is on-premise, use IPsec. Hosted Exchange automatically secures the connection by using SSL.

Use the principle of least privileges for the connector

For a list of the minimum cmdlets that the Exchange Server connector requires, see Manage mobile devices with Configuration Manager and Exchange.

Security best practices for Macs

Store and access the client source files from a secured location

Before installing or enrolling the client on Mac computer, Configuration Manager doesn't verify whether these client source files have been tampered with. Download these files from a trustworthy source. Securely store and access them.

Monitor and track the validity period of the certificate

To ensure business continuity, monitor and track the validity period of the certificates that you use for Mac computers. Configuration Manager doesn't support automatic renewal of this certificate, or warn you that the certificate is about to expire. A typical validity period is one year.

For more information about how to renew the certificate, see Renewing the Mac client certificate manually.

Configure the trusted root certificate for SSL only

To help protect against elevation of privileges, configure the certificate for the trusted root certificate authority so that it's only trusted for the SSL protocol.

When you enroll Mac computers, a user certificate to manage the Configuration Manager client is automatically installed. This user certificate includes the trusted root certificates in its trust chain. To restrict the trust of this root certificate to the SSL protocol only, use the following procedure:

1. On the Mac computer, open a terminal window.
2. Enter the following command:
   ```
   sudo /Applications/Utilities/Keychain\ Access.app/Contents/MacOS/Keychain\ Access
   ```
3. In the **Keychain Access** dialog box, in the **Keychains** section, click **System**. Then in the **Category** section, click **Certificates**.
4. Locate and double-click the root CA certificate for the Mac client certificate.

5. In the dialog box for the root CA certificate, expand the **Trust** section, and then make the following changes:

    a. **When using this certificate**: Change the **Always Trust** setting to **Use System Defaults**.

    b. **Secure Sockets Layer (SSL)**: Change **no value specified** to **Always Trust**.

6. Close the dialog box. When prompted, enter the administrator's password, and then click **Update Settings**.

After you complete this procedure, the root certificate is only trusted to validate the SSL protocol. Other protocols that are now untrusted with this root certificate include Secure Mail (S/MIME), Extensible Authentication (EAP), or code signing.

> **NOTE**
> Also use this procedure if you installed the client certificate independently from Configuration Manager.

Security issues for Configuration Manager clients

The following security issues have no mitigation:

Status messages aren't authenticated

No authentication is performed on status messages. When a management point accepts HTTP client connections, any device can send status messages to the management point. If the management point accepts HTTPS client connections only, a device must have a valid client authentication certificate, but could also send any status message. The management point discards any invalid status message received from a client.

There are a few potential attacks against this vulnerability:

- An attacker could send a bogus status message to gain membership in a collection that's based on status message queries.
- Any client could launch a denial of service against the management point by flooding it with status messages.
- If status messages are triggering actions in status message filter rules, an attacker could trigger the status message filter rule.
- An attacker could send status message that would render reporting information inaccurate.

Policies can be retargeted to non-targeted clients

There are several methods that attackers could use to make a policy targeted to one client apply to an entirely different client. For example, an attacker at a trusted client could send false inventory or discovery information to have the computer added to a collection to which it shouldn't belong. That client then receives all the deployments to that collection.

Controls exist to help prevent attackers from directly modifying policy. However, attackers could take an existing policy that reformats and redeploys an OS and send it to a different computer. This redirected policy could create a denial of service. These types of attacks would require precise timing and extensive knowledge of the Configuration Manager infrastructure.

Client logs allow user access

All the client log files allow the **Users** group with *Read* access, and the special **Interactive** user with *Write* access. If you enable verbose logging, attackers might read the log files to look for information about compliance or system vulnerabilities. Processes such as software that the client installs in a user's context must write to logs with a low-rights user account. This behavior means an attacker could also write to the logs with a low-rights account.

The most serious risk is that an attacker could remove information in the log files. An administrator might need this information for auditing and intrusion detection.

A computer could be used to obtain a certificate that's designed for mobile device enrollment

When Configuration Manager processes an enrollment request, it can't verify the request originated from a mobile device rather than from a computer. If the request is from a computer, it can install a PKI certificate that then allows it to register with Configuration Manager.

To help prevent an elevation of privilege attack in this scenario, only allow trusted users to enroll their mobile devices. Carefully monitor device enrollment activities in the site.

A blocked client can still send messages to the management point

When you block a client that you no longer trust, but it established a network connection for client notification, Configuration Manager doesn't disconnect the session. The blocked client can continue to send packets to its management point until the client disconnects from the network. These packets are only small, keep-alive packets. This client can't be managed by Configuration Manager until it's unblocked.

Automatic client upgrade doesn't verify the management point

When you use automatic client upgrade, the client can be directed to a management point to download the client source files. In this scenario, the client doesn't verify the management point as a trusted source.

When users first enroll Mac computers, they're at risk from DNS spoofing

When the Mac computer connects to the enrollment proxy point during enrollment, it's unlikely that the Mac computer already has the trusted root CA certificate. At this point, the Mac computer doesn't trust the server, and prompts the user to continue. If a rogue DNS server resolves the fully qualified domain name (FQDN) of the enrollment proxy point, it could direct the Mac computer to a rogue enrollment proxy point to install certificates from an untrusted source. To help reduce this risk, follow best practices to avoid DNS spoofing in your environment.

Mac enrollment doesn't limit certificate requests

Users can re-enroll their Mac computers, each time requesting a new client certificate. Configuration Manager doesn't check for multiple requests or limit the number of certificates requested from a single computer. A rogue user could run a script that repeats the command-line enrollment request. This attack could cause a denial of service on the network or on the issuing certificate authority (CA). To help reduce this risk, carefully monitor the issuing CA for this type of suspicious behavior. Immediately block from the Configuration Manager hierarchy any computer that shows this pattern of behavior.

A wipe acknowledgment doesn't verify that the device has been successfully wiped

When you initiate a wipe action for a mobile device, and Configuration Manager acknowledges the wipe, the verification is that Configuration Manager successfully *sent* the message. It doesn't verify that the device *acted* on the request.

For mobile devices managed by the Exchange Server connector, a wipe acknowledgment verifies that the command was received by Exchange, not by the device.

If you use the options to commit changes on Windows Embedded devices, accounts might be locked out sooner than expected

If the Windows Embedded device is running an OS version prior to Windows 7, and a user attempts to sign in while the write filters are disabled by Configuration Manager, Windows allows only half of the configured number of incorrect attempts before the account is locked out.

For example, you configure the domain policy for **Account lockout threshold** to six attempts. A user mistypes their password three times, and the account is locked out. This behavior effectively creates a denial of service. If users must sign in to embedded devices in this scenario, caution them about the potential for a reduced lockout threshold.

Privacy information for Configuration Manager clients

When you deploy the Configuration Manager client, you enable client settings for Configuration Manager features.

The settings that you use to configure the features can apply to all clients in the Configuration Manager hierarchy. This behavior is the same whether they're directly connected to the internal network, connected through a remote session, or connected to the internet.

Client information is stored in the Configuration Manager database in your SQL server, and isn't sent to Microsoft. Information is retained in the database until it's deleted by the site maintenance tasks **Delete Aged Discovery Data** every 90 days. You can configure the deletion interval.

Some summarized or aggregate diagnostics and usage data is sent to Microsoft. For more information, see Diagnostics and usage data.

Before you configure the Configuration Manager client, consider your privacy requirements.

You can learn more about Microsoft's data collection and use in the Microsoft Privacy Statement.

Client status

Configuration Manager monitors the activity of clients. It periodically evaluates the Configuration Manager client and can remediate issues with the client and its dependencies. Client status is enabled by default. It uses server-side metrics for the client activity checks. Client status uses client-side actions for self-checks, remediation, and for sending client status information to the site. The client runs the self-checks according to a schedule that you configure. The client sends the results of the checks to the Configuration Manager site. This information is encrypted during transfer.

Client status information is stored in the Configuration Manager database in your SQL server, and isn't sent to Microsoft. The information isn't stored in encrypted format in the site database. This information is retained in the database until it's deleted according to the value configured for the **Retain client status history for the following number of days** client status setting. The default value for this setting is every 31 days.

Before you install the Configuration Manager client with client status checking, consider your privacy requirements.

Privacy information for mobile devices that are managed with the Exchange Server Connector

The Exchange Server Connector finds and manages devices that connect to an on-premises or hosted Exchange Server by using the ActiveSync protocol. The records found by the Exchange Server Connector are stored in the Configuration Manager database in your SQL server. The information is collected from the Exchange Server. It doesn't contain any additional information from what the mobile devices send to Exchange Server.

The mobile device information isn't sent to Microsoft. The mobile device information is stored in the Configuration Manager database in your SQL server. Information is retained in the database until it's deleted by the site maintenance task **Delete Aged Discovery Data** every 90 days. You configure the deletion interval.

Before you install and configure the Exchange Server connector, consider your privacy requirements.

You can learn more about Microsoft's data collection and use in the Microsoft Privacy Statement.

Best practices for client deployment in System Center Configuration Manager

2/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use software update-based client installation for Active Directory computers

This client deployment method uses existing Windows technologies, integrates with your Active Directory infrastructure, requires the least configuration in Configuration Manager, is the easiest to configure for firewalls, and is the most secure. By using security groups and WMI filtering for the Group Policy configuration, you also have a lot of flexibility to control which computers install the Configuration Manager client.

For more information, see How to Install Configuration Manager Clients by Using Software Update-Based Installation.

Extend the Active Directory schema and publish the site so that you can run CCMSetup without command-line options

When you extend the Active Directory schema for Configuration Manager and the site is published to Active Directory Domain Services, many client installation properties are published to Active Directory Domain Services. If a computer can locate these client installation properties, it can use them during Configuration Manager client deployment. Because this information is automatically generated, the risk of human error associated with manually entering installation properties is eliminated.

For more information, see About client installation properties published to Active Directory Domain Services in System Center Configuration Manager.

Use a phased rollout to manage CPU usage

Minimize the effect of the CPU processing requirements on the site server by using a phased rollout of clients. Deploy clients outside business hours so that other services have more available bandwidth during the day and users are not disrupted if their computer slows down or requires a restart.

Enable automatic upgrade after your main client deployment has finished

Automatic client upgrades are useful when you want to upgrade a small number of client computers that might have been missed by your main client installation method, perhaps because they were offline.

> **NOTE**
> Performance improvements in Configuration Manager can allow you to use automatic upgrades as a primary client upgrade method. However, performance will depend on your hierarchy infrastructure, such as the number of clients.

Use SMSMP and FSP if you install the client with client.msi properties

The SMSMP property specifies the initial management point for the client to communicate with and removes the dependency on service location solutions such as Active Directory Domain Services, DNS, and WINS.

Use the FSP property and install a fallback status point so that you can monitor client installation and assignment, and identify any communication problems.

For more information about these options, see About client installation properties in System Center Configuration Manager.

Install client language packs before you install the clients

We recommend that you install client language packs before deploying the client. If you install client language packs (to enable additional languages) on a site after you install clients, you must reinstall the clients before they can use those languages. For mobile device clients, you must wipe the mobile device and enroll it again.

Prepare required PKI certificates in advance

To manage devices on the Internet, enrolled mobile devices, and Mac computers, you must have PKI certificates on site systems (management points and distribution points) and the client devices. On production networks, you might require change management approval to use new certificates, restart site system servers, or users might have to logoff and logon for new group membership. In addition, you might have to allow sufficient time for replication of security permissions and for any new certificate templates.

For more information about required PKI certificates, see PKI certificate requirements for System Center Configuration Manager.

Before you install clients, configure any required client settings and maintenance windows

Although you can configure client settings and maintenance windows before or after clients are installed, it's better to configure required settings before you install clients so that they are used as soon as the client is installed.

Configure maintenance windows for servers and for Windows Embedded devices to ensure business continuity for critical devices. Maintenance windows will ensure that required software updates and antimalware software do not restart the computer during business hours.

> **IMPORTANT**
>
> For Windows 10 computers that you plan to protect with Unified Write Filter (UWF), you must configure the device for UWF before you install the client. This enables Configuration Manager to install the client with a custom credential provider that locks out low-rights users from logging in to the device during maintenance mode.

Plan your user enrollment experience for Mac computers and mobile devices

If users will enroll their own Mac computers and mobile devices with Configuration Manager, plan the user experience. For example, you might script the installation and enrollment process by using a web page so users enter the minimum amount of information necessary, and send instructions with a link by email.

Use File-Based Write Filters for Windows Embedded devices

Embedded devices that use Enhanced Write Filters (EWF) are likely to experience state message resynchronizations. If you have just a few embedded devices that use Enhanced Write Filters, you might not notice this. However, when you have a lot of embedded devices that resynchronize their information, such as sending full

inventory rather than delta inventory, this can generate a noticeable increase in network packets and higher CPU processing on the site server.

When you have a choice of which type of write filter to enable, choose File-Based Write Filters and configure exceptions to persist client state and inventory data between device restarts for network and CPU efficiency on the Configuration Manager client. For more information about write filters, see Planning for client deployment to Windows Embedded devices in System Center Configuration Manager.

For more information about the maximum number of Windows Embedded clients that a primary site can support, see Supported operating sysetms for clients and devices.

Determine whether to block clients in System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

If a client computer or client mobile device is no longer trusted, you can block the client in the System Center 2012 Configuration Manager console. Blocked clients are rejected by the Configuration Manager infrastructure so that they cannot communicate with site systems to download policy, upload inventory data, or send state or status messages.

You must block and unblock a client from its assigned site rather than from a secondary site or a central administration site.

> **IMPORTANT**
> Although blocking in Configuration Manager can help to secure the Configuration Manager site, do not rely on this feature to protect the site from untrusted computers or mobile devices if you allow clients to communicate with site systems by using HTTP, because a blocked client could rejoin the site with a new self-signed certificate and hardware ID. Instead, use the blocking feature to block lost or compromised boot media that you use to deploy operating systems, and when site systems accept HTTPS client connections.

Clients that access the site by using the ISV Proxy certificate cannot be blocked. For more information about the ISV Proxy certificate, see the System Center Configuration Manager Software Development Kit (SDK).

If your site systems accept HTTPS client connections and your public key infrastructure (PKI) supports a certificate revocation list (CRL), always consider certificate revocation to be the primary line of defense against potentially compromised certificates. Blocking clients in Configuration Manager offers a second line of defense to protect your hierarchy.

Considerations for blocking clients

- This option is available for HTTP and HTTPS client connections, but has limited security when clients connect to site systems by using HTTP.
- Configuration Manager administrative users have the authority to block a client, and the action is taken in the Configuration Manager console.
- Client communication is rejected from the Configuration Manager hierarchy only.

  > **NOTE**
  > The same client could register with a different Configuration Manager hierarchy.

- The client is immediately blocked from the Configuration Manager site.
- Helps to protect site systems from potentially compromised computers and mobile devices.

Considerations for using certificate revocation

- This option is available for HTTPS Windows client connections if the public key infrastructure supports a

certificate revocation list (CRL).

Mac clients always perform CRL checking and this functionality cannot be disabled.

Although mobile device clients do not use certificate revocation lists to check the certificates for site systems, their certificates can be revoked and checked by Configuration Manager.

- Public key infrastructure administrators have the authority to revoke a certificate, and the action is taken outside the Configuration Manager console.
- Client communication can be rejected from any computer or mobile device that requires this client certificate.
- There is likely to be a delay between revoking a certificate and site systems downloading the modified certificate revocation list (CRL).
- For many PKI deployments, this delay can be a day or longer. For example, in Active Directory Certificate Services, the default expiration period is one week for a full CRL, and one day for a delta CRL.
- Helps to protect site systems and clients from potentially compromised computers and mobile devices.

> **NOTE**
> You can further protect site systems that run IIS from unknown clients by configuring a certificate trust list (CTL) in IIS.

Planning for client deployment to Linux and UNIX computers in Configuration Manager

3/27/2019 • 10 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

IMPORTANT

Starting in version 1902, Configuration Manager doesn't support Linux or UNIX clients.

Consider Microsoft Azure Management for managing Linux servers. Azure solutions have extensive Linux support that in most cases exceed Configuration Manager functionality, including end-to-end patch management for Linux.

You can install the Configuration Manager client on computers that run Linux or UNIX. This client is designed for servers that operate as a workgroup computer, and the client doesn't support interaction with logged-on users. After you install the client software and the client establishes communication with the Configuration Manager site, you manage the client by using the Configuration Manager console and reports.

NOTE

The Configuration Manager client for Linux and UNIX computers does not support the following management capabilities:

- Client push installation
  - Operating system deployment
  - Application deployment; instead, deploy software by using packages and programs.
  - Software inventory
  - Software updates
  - Compliance settings
  - Remote control
  - Power management
  - Client status client check and remediation
  - Internet-based client management

For information about the supported Linux and UNIX distributions and the hardware required to support the client for Linux and UNIX, see Recommended hardware for System Center Configuration Manager.

Use the information in this article to help you plan to deploy the Configuration Manager client for Linux and UNIX.

Prerequisites for Client Deployment to Linux and UNIX Servers

Use the following information to determine the prerequisites you must have in place to successfully install the client for Linux and UNIX.

Dependencies External to Configuration Manager:

The following tables describe the required UNIX and Linux operating systems and package dependencies.

Red Hat Enterprise Linux Server release 5.1 (Tikanga)

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
glibc	C Standard Libraries	2.5-12
Openssl	OpenSSL Libraries; Secure Network Communications Protocol	0.9.8b-8.3.el5
PAM	Pluggable Authentication Modules	0.99.6.2-3.14.el5

Red Hat Enterprise Linux Server release 6

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
glibc	C Standard Libraries	2.12-1.7
Openssl	OpenSSL Libraries; Secure Network Communications Protocol	1.0.0-4
PAM	Pluggable Authentication Modules	1.1.1-4

Red Hat Enterprise Linux Server release 7

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
glibc	C Standard Libraries	2.17
Openssl	OpenSSL Libraries; Secure Network Communications Protocol	1.0.1
PAM	Pluggable Authentication Modules	1.1.1-4

Solaris 10 SPARC

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
Required operating system patch	PAM memory leak	117463-05
SUNWlibC	Sun Workshop Compilers Bundled libC (sparc)	5.10, REV=2004.12.22
SUNWlibms	Math & Microtasking Libraries (Usr) (sparc)	5.10, REV=2004.11.23
SUNWlibmsr	Math & Microtasking Libraries (Root) (sparc)	5.10, REV=2004.11.23
SUNWcslr	Core Solaris Libraries (Root) (sparc)	11.10.0, REV=2005.01.21.15.53
SUNWcsl	Core Solaris Libraries (Root) (sparc)	11.10.0, REV=2005.01.21.15.53

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
OpenSSL	SUNopenssl-librararies (Usr) Sun provides the OpenSSL libraries for Solaris 10 SPARC. They are bundled with the operating system.	11.10.0,REV=2005.01.21.15.53
PAM	Pluggable Authentication Modules SUNWcsr, Core Solaris, (Root) (sparc)	11.10.0, REV=2005.01.21.15.53

Solaris 10 x86

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
Required operating system patch	PAM memory leak	117464-04
SUNWlibC	Sun Workshop Compilers Bundled libC (i386)	5.10,REV=2004.12.20
SUNWlibmsr	Math & Microtasking Libraries (Root) (i386)	5.10, REV=2004.12.18
SUNWcsl	Core Solaris, (Shared Libs) (i386)	11.10.0,REV=2005.01.21.16.34
SUNWcslr	Core Solaris Libraries (Root) (i386)	11.10.0, REV=2005.01.21.16.34
OpenSSL	SUNWopenssl-libraries; OpenSSL Libraries (Usr) (i386)	11.10.0, REV=2005.01.21.16.34
PAM	Pluggable Authentication Modules SUNWcsr Core Solaris, (Root)(i386)	11.10.0,REV=2005.01.21.16.34

Solaris 11 SPARC

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
SUNWlibC	Sun Workshop Compilers Bundled libC	5.11, REV=2011.04.11
SUNWlibmsr	Math & Microtasking Libraries (Root)	5.11, REV=2011.04.11
SUNWcslr	Core Solaris Libraries (Root)	11.11, REV=2009.11.11
SUNWcsl	Core Solaris, (Shared Libs)	11.11, REV=2009.11.11
SUNWcsr	Core Solaris, (Root)	11.11, REV=2009.11.11
SUNWopenssl-libraries	OpenSSL Libraries (Usr)	11.11.0,REV=2010.05.25.01.00

Solaris 11 x86

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
SUNWlibC	Sun Workshop Compilers Bundled libC	5.11, REV=2011.04.11
SUNWlibmsr	Math & Microtasking Libraries (Root)	5.11, REV=2011.04.11
SUNWcslr	Core Solaris Libraries (Root)	11.11, REV=2009.11.11
SUNWcsl	Core Solaris, (Shared Libs)	11.11, REV=2009.11.11
SUNWcsr	Core Solaris, (Root)	11.11, REV=2009.11.11
SUNWopenssl-libraries	OpenSSL Libraries (Usr)	11.11.0,REV=2010.05.25.01.00

SUSE Linux Enterprise Server 10 SP1 (i586)

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
glibc-2.4-31.30	C Standard shared library	2.4-31.30
OpenSSL	OpenSSL Libraries; Secure Network Communications Protocol	0.9.8a-18.15
PAM	Pluggable Authentication Modules	0.99.6.3-28.8

SUSE Linux Enterprise Server 11 (i586)

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
glibc-2.9-13.2	C Standard shared library	2.9-13.2
PAM	Pluggable Authentication Modules	pam-1.0.2-20.1

Universal Linux (Debian package) Debian, Ubuntu Server

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
libc6	C Standard shared library	2.3.6
OpenSSL	OpenSSL Libraries; Secure Network Communications Protocol	0.9.8 or 1.0
PAM	Pluggable Authentication Modules	0.79-3

Universal Linux (RPM package) CentOS, Oracle Linux

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
glibc	C Standard shared library	2.5-12
OpenSSL	OpenSSL Libraries; Secure Network Communications Protocol	0.9.8 or 1.0

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
PAM	Pluggable Authentication Modules	0.99.6.2-3.14

IBM AIX 6.1

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
OS version	Version of operating system	AIX 6.1: any Technology Level and Service Pack
xlC.rte	XL C/C++ Runtime	9.0.0.5
OpenSSL/openssl.base	OpenSSL Libraries; Secure Network Communications Protocol	0.9.8.4

IBM AIX 7.1 (Power)

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
OS version	Version of operating system	AIX 7.1: any Technology Level and Service Pack
xlC.rte	XL C/C++ Runtime	
OpenSSL/openssl.base	OpenSSL Libraries; Secure Network Communications Protocol	

HP-UX 11i v3 IA64

REQUIRED PACKAGE	DESCRIPTION	MINIMUM VERSION
HPUX11i-OE	HP-UX Foundation Operating Environment	B.11.31.0709
OS-Core.MinimumRuntime.CORE-SHLIBS	Specific IA development libraries	B.11.31
SysMgmtMin	Minimum Software Deployment Tools	B.11.31.0709
SysMgmtMin.openssl	OpenSSL Libraries; Secure Network Communications Protocol	A.00.09.08d.002
PAM	Pluggable Authentication Modules	On HP-UX, PAM is part of the core operating system components. There are no other dependencies.

Configuration Manager Dependencies: The following table lists site system roles that support Linux and UNIX clients. For more information about these site system roles, see Determine the site system roles for System Center Configuration Manager clients.

CONFIGURATION MANAGER SITE SYSTEM	MORE INFORMATION

CONFIGURATION MANAGER SITE SYSTEM	MORE INFORMATION
Management point	Although a management point isn't required to install a Configuration Manager client for Linux and UNIX, you must have a management point to transfer information between client computers and Configuration Manager servers. Without a management point, you can't manage client computers.
Distribution point	The distribution point isn't required to install a Configuration Manager client for Linux and UNIX. However, the site system role is required if you deploy software to Linux and UNIX servers. Because the Configuration Manager client for Linux and UNIX doesn't support communications that use SMB, the distribution points you use with the client must support HTTP or HTTPS communication.
Fallback status point	The fallback status point isn't required to install a Configuration Manager client for Linux and UNIX. However, The fallback status point enables computers in the Configuration Manager site to send state messages when they can't communicate with a management point. Client can also send their installation status to the fallback status point.

Firewall Requirements: Ensure that firewalls don't block communications across the ports you specify as client request ports. The client for Linux and UNIX communicates directly with management points, distribution points, and fallback status points.

For information about client communication and request ports, see Configure the Client for Linux and UNIX to Locate Management Points.

Planning for Communication across Forest Trusts for Linux and UNIX Servers

Linux and UNIX servers you manage with Configuration Manager operate as workgroup clients and require similar configurations as Windows-based clients that are in a workgroup. For information about communications from computers that are in workgroups, see Communications across Active Directory forests.

Service Location by the client for Linux and UNIX

The task of locating a site system server that provides service to clients is referred to as service location. Unlike a Windows-based client, the client for Linux and UNIX doesn't use Active Directory for service location. Additionally, the Configuration Manager client for Linux and UNIX doesn't support a client property that specifies the domain suffix of a management point. Instead, the client learns about additional site system servers that provide services to clients from a known management point you assign when you install the client software.

For more information, see Service Location and how clients determine their assigned management point.

Planning for Security and Certificates for Linux and UNIX Servers

For secure and authenticated communications with Configuration Manager sites, the Configuration Manager client for Linux and UNIX uses the same model for communication as the Configuration Manager client for Windows.

When you install the Linux and UNIX client, you can assign the client a PKI certificate that enables it to use HTTPS to communicate with Configuration Manager sites. If you don't assign a PKI certificate, the client creates a self-signed certificate and communicates only by HTTP.

Clients that are provided a PKI certificate when they install use HTTPS to communicate with management points. When a client is unable to locate a management point that supports HTTPS, it will fall back to use HTTP with the provided PKI certificate.

When a Linux or UNIX client uses a PKI certificate, you don't have to approve them. When a client uses a self-signed certificate, review the hierarchy settings for client approval in the Configuration Manager console. If the client approval method is not **Automatically approve all computers (not recommended)**, you must manually approve the client.

For more information about how to manually approve the client, see Manage clients from the devices node.

For information about how to use certificates in Configuration Manager, see PKI certificate requirements.

About Certificates for use by Linux and UNIX Servers

The Configuration Manager client for Linux and UNIX uses a self-signed certificate or an X.509 PKI certificate just like Windows-based clients. There are no changes to the PKI requirements for Configuration Manager site systems when you manage Linux and UNIX clients.

The certificates you use for Linux and UNIX clients that communicate to Configuration Manager site systems must be in a Public Key Certificate Standard (PKCS#12) format, and the password must be known so you can specify it to the client when you specify the PKI certificate.

The Configuration Manager client for Linux and UNIX supports a single PKI certificate, and doesn't support multiple certificates. Therefore, the certificate selection criteria you configure for a Configuration Manager site doesn't apply.

Configuring Certificates for Linux and UNIX Servers

To configure a Configuration Manager client for Linux and UNIX servers to use HTTPS communications, you must configure the client to use a PKI certificate at the time you install the client. You can't provision a certificate before installation of the client software.

When you install a client that uses a PKI certificate, you use the command-line parameter `-UsePKICert` to specify the location and name of a PKCS#12 file that contains the PKI certificate. Additionally you must use the command-line parameter `-certpw` to specify the password for the certificate.

If you don't specify `-UsePKICert`, the client generates a self-signed certificate and attempts to communicate to site system servers by using HTTP only.

Versions that don't support SHA-256

The following Linux and UNIX operating systems that are supported as clients for Configuration Manager were released with versions of OpenSSL that don't support SHA-256:

- Solaris Version 10 (SPARC/x86)

To manage these operating systems with Configuration Manager, you must install the Configuration Manager client for Linux and UNIX with a command-line switch that directs the client to skip validation of SHA-256. Configuration Manager clients that run on these operating system versions operate in a less secure mode than clients that support SHA-256. This less secure mode of operation has the following behavior:

- Clients don't validate the site server signature associated with policy they request from a management point.
- Clients don't validate the hash for packages that they download from a distribution point.

IMPORTANT

The `ignoreSHA256validation` option allows you to run the client for Linux and UNIX computers in a less secure mode. This is intended for use on older platforms that did not include support for SHA-256. This is a security override and is not recommended by Microsoft, but is supported for use in a secure and trusted datacenter environment.

When the Configuration Manager client for Linux and UNIX installs, the install script checks the operating system version. By default, if the operating system version is identified as having released without a version of OpenSSL that supports SHA-256, the installation of the Configuration Manager client fails.

To install the Configuration Manager client on Linux and UNIX operating systems that didn't release with a version of OpenSSL that supports SHA-256, you must use the install command-line switch `ignoreSHA256validation`. When you use this command-line option on an applicable Linux or UNIX operating system, the Configuration Manager client will skip SHA-256 validation and after installation, the client won't use SHA-256 to sign data it submits to site systems by using HTTP. For information about configuring Linux and UNIX clients to use certificates, see Planning for Security and Certificates for Linux and UNIX Servers. For more information about requiring SHA-256, see Configure signing and encryption.

NOTE

The command line option `ignoreSHA256validation` is ignored on computers that run a version of Linux and UNIX that released with versions of OpenSSL that support SHA-256.

Planning for client deployment to Mac computers in System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can install the Configuration Manager client on Mac computers that run the Mac OS X operating system and use the following management capabilities:

- **Hardware inventory**

  You can use Configuration Manager hardware inventory to collect information about the hardware and installed applications on Mac computers. This information can then be viewed in Resource Explorer in the Configuration Manager console and used to create collections, queries and reports. For more information, see How to use Resource Explorer to view hardware inventory in System Center Configuration Manager.

  Configuration Manager collects the following hardware information from Mac computers:

  - Processor
  - Computer System
  - Disk Drive
  - Disk Partition
  - Network Adapter
  - Operating System
  - Service
  - Process
  - Installed Software
  - Computer System Product
  - USB Controller
  - USB Device
  - CDROM Drive
  - Video Controller
  - Desktop Monitor
  - Portable Battery
  - Physical Memory
  - Printer

> **IMPORTANT**
> You cannot extend the hardware information that is collected from Mac computers during hardware inventory.

- **Compliance settings**

  You can use Configuration Manager compliance settings to view the compliance of and remediate Mac OS X preference (.plist) settings. For example, you could enforce settings for the home page in the Safari web browser or ensure that the Apple firewall is enabled. You can also use shell scripts to monitor and remediate settings in MAC OS X.

- **Application management**

  Configuration Manager can deploy software to Mac computers. You can deploy the following software formats to Mac computers:

  - Apple Disk Image (.DMG)
  - Meta Package File (.MPKG)
  - Mac OS X Installer Package (.PKG)
  - Mac OS X Application (.APP)

  When you install the Configuration Manager client on Mac computers, you cannot use the following management capabilities that are supported by the Configuration Manager client on Windows-based computers:

- Client push installation
- Operating system deployment
- Software updates

  > **NOTE**
  > You can use Configuration Manager application management to deploy required Mac OS X software updates to Mac computers. In addition, you can use compliance settings to make sure that computers have any required software updates.

- Maintenance windows
- Remote control
- Power management
- Client status client check and remediation

  For more information about how to install and configure the Configuration Manager Mac client, see How to deploy clients to Macs in System Center Configuration Manager.

Planning for client deployment to Windows Embedded devices in System Center Configuration Manager

9/5/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

If your Windows Embedded device does not include the System Center Configuration Manager client, you can use any of the client installation methods if the device meets the required dependencies. If the embedded device supports write filters, you must disable these filters before you install the client, and then re-enable the filters again after the client is installed and assigned to a site.

Note that when you disable the filters, you should not disable the filter drivers. Typically these drivers are started automatically when the computer is started. Disabling the drivers will either prevent installation of the client, or interfere with write filter orchestration which will cause client operations to fail. These are the services associated with each write filter type that must remain running:

WRITE FILTER TYPE	DRIVER	TYPE	DESCRIPTION
EWF	ewf	Kernel	Implements sector-level I/O redirection on protected volumes.
FBWF	fbwf	File system	Implements file-level I/O redirection on protected volumes.
UWF	uwfreg	Kernel	UWF Registry Redirector
UWF	uwfs	File System	UWF File Redirector
UWF	uwfvol	Kernel	UWF Volume Manager

Write filters control how the operating system on the embedded device is updated when you make changes, such as when you install software. When write filters are enabled, instead of making the changes directly to the operating system, these changes are redirected to a temporary overlay. If the changes are only written to the overlay, they are lost when the embedded device shuts downs. However, if the write filters are temporarily disabled, the changes can be made permanent so that you do not have to make the changes again (or reinstall software) every time that the embedded device restarts. However, temporarily disabling and then re-enabling the write filters requires one or more restarts, so that you typically want to control when this happens by configuring maintenance windows so that restarts occur outside business hours.

You can configure options to automatically disable and re-enable the write filters when you deploy software such as applications, task sequences, software updates, and the Endpoint Protection client. The exception is for configuration baselines with configuration items that use automatic remediation. In this scenario, the remediation always occurs in the overlay so that it is available only until the device is restarted. The remediation is applied again at the next evaluation cycle, but only to the overlay, which is cleared at restart. To force Configuration Manager to commit the remediation changes, you can deploy the configuration baseline and then another software deployment that supports committing the change as soon as possible.

If the write filters are disabled, you can install software on Windows Embedded devices by using Software Center. However, if the write filters are enabled, the installation fails and Configuration Manager displays an error message that you have insufficient permissions to install the application.

> **WARNING**
> Even if you do not select the Configuration Manager options to commit the changes, the changes might be committed if another software installation or change is made that commits changes. In this scenario, the original changes will be committed in addition to the new changes.

When Configuration Manager disables the write filters to make changes permanent, only users who have local administrative rights can log on and use the embedded device. During this period, low-rights users are locked out and see a message that the computer is unavailable because it is being serviced. This helps protect the device while it is in a state where changes can be permanently applied, and this servicing mode lockout behavior is another reason to configure a maintenance window for a time when users will not log on to these devices.

Configuration Manager supports managing the following types of write filters:

- File-Based Write Filter (FBWF) - For more information, see File-Based Write Filter.
- Enhanced Write Filter (EWF) RAM - For more information, see Enhanced Write Filter.
- Unified Write Filter (UWF) - For more information, see Unified Write Filter.

  Configuration Manager does not support write filter operations when the Windows Embedded device is in EWF RAM Reg mode.

IMPORTANT

If you have the choice, use File-Based Write Filters (FBWF) with Configuration Manager for increased efficiency and higher scalability.

For devices that use FBWF only: Configure the following exceptions to persist client state and inventory data between device restarts:

- CCMINSTALLDIR*.sdf
  - CCMINSTALLDIR\ServiceData
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM\StateSystem

  Devices that run Windows Embedded 8.0 and later do not support exclusions that contain wildcard characters. On these devices, you must configure the following exclusions individually:

- All files in CCMINSTALLDIR with the extension .sdf, typically:
  - UserAffinityStore.sdf
  - InventoryStore.sdf
  - CcmStore.sdf
  - StateMessageStore.sdf
  - CertEnrollmentStore.sdf
  - CCMINSTALLDIR\ServiceData
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM\StateSystem

For devices that use FBWF and UWF only: When clients in a workgroup use certificates for authentication to management points, you must also exclude the private key to ensure the client continues to communicate with the management point. On these devices, configure the following exceptions:

- c:\Windows\System32\Microsoft\Protect
  - c:\ProgramData\Microsoft\Crypto
  - HKEY_LOCAL_MACHINE\Software\Microsoft\SystemCertificates\SMS\Certificates

NOTE

No additional exceptions are needed by the Configuration Manager client other than those documented in the above **Important** box. Adding additional Configuration Manager or WMI (WBEM) related exceptions may lead to failures of the Configuration Manager including devices getting stuck in servicing mode or devices experiencing reboot loops. Unneeded exceptions include the Configuration Manager client directory, the CCMcache directory, the CCMSetup directory, the Task Sequence cache directory, the WBEM directory, and Configuration Manager related registry keys.

For an example scenario to deploy and manage write-filter-enabled Windows Embedded devices in Configuration Manager see Example scenario for deploying and managing System Center Configuration Manager clients on Windows Embedded devices.

For more information about how to build images for Windows Embedded devices and configure write filters, see your Windows Embedded documentation, or contact your OEM.

NOTE

When you select the applicable platforms for software deployments and configuration items, these display the Windows Embedded families rather than specific versions. Use the following list to map the specific version of Windows Embedded to the options in the list box:

- **Embedded Operating Systems based on Windows XP (32-bit)** includes the following:
  - Windows XP Embedded
  - Windows Embedded for Point of Service
  - Windows Embedded Standard 2009
  - Windows Embedded POSReady 2009
  - **Embedded operating systems based on Windows 7 (32-bit)** includes the following:
  - Windows Embedded Standard 7 (32-bit)
  - Windows Embedded POSReady 7 (32-bit)
  - Windows ThinPC
  - **Embedded operating systems based on Windows 7 (64-bit)** includes the following:
  - Windows Embedded Standard 7 (64-bit)
  - Windows Embedded POSReady 7 (64-bit)

Example scenario for deploying and managing System Center Configuration Manager clients on Windows Embedded devices

5/20/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This scenario demonstrates how you can manage write-filter-enabled Windows Embedded devices with Configuration Manager.If your embedded devices do not support write filters, they behave as standard Configuration Manager clients and these procedures don't apply.

Coho Vineyard & Winery is opening a visitor center and needs kiosks that run Windows Embedded to run interactive presentations. The building for the new visitor center is not close to the IT department, so the kiosks must be managed remotely. In addition to the software that runs the presentations, these devices must run up-to-date antimalware protection software to comply with the company security policies. The kiosks must run 7 days a week, with no downtime while the visitor center is open.

Coho already runs Configuration Manager to manage devices on their network. Configuration Manager is configured to run Endpoint Protection, and install software updates and applications. However, because the IT team has not managed Windows Embedded devices before, the Configuration Manager administrator runs a pilot to manage two kiosks in the reception lobby.

To manage these Windows Embedded devices that are write-filter-enabled, Configuration Manager administrator performs the following steps to install the Configuration Manager client, protect the client by using Endpoint Protection, and install the interactive presentation software.

1. The Configuration Manager administrator (the Admin) reads how Windows Embedded devices uses write filters and how Configuration Manager can make this easier by automatically disabling and then re-enabling the writer filters to persist a software installation.

   For more information, see Planning for client deployment to Windows Embedded devices in System Center Configuration Manager.

2. Before the Admin installs the Configuration Manager client, the Admin creates a new query-based device collection for the Windows Embedded devices. Because the company uses standard naming formats to identify their computers, the Admin can uniquely identify Windows Embedded devices by the first six letters of the computer name: **WEMDVC**. The Admin uses the following WQL query to create this collection: **select SMS_R_System.NetbiosName from SMS_R_System where SMS_R_System.NetbiosName like "WEMDVC%"**

   This collection allows the Admin to manage the Windows Embedded devices with different configuration options from the other devices. The Admin will use this collection to control restarts, deploy Endpoint Protection with client settings, and deploy the interactive presentation application.

   See How to create collections in System Center Configuration Manager.

3. The Admin configures the collection for a maintenance window to ensure that restarts that might be required for installing the presentation application and any upgrades do not occur during opening hours for the visitor center. Opening hours will be 09:00 through 18:00, Monday through Sunday. The Admin configures the maintenance window for every day, 18:30 through 06:00.

4. For more information, see How to use maintenance windows in System Center Configuration Manager.

5. The Admin then configures a custom device client setting to install the Endpoint Protection client by selecting **Yes** for the following settings, and then deploys this custom client setting to the Windows Embedded device collection:

   - **Install Endpoint Protection client on client computers**
   - **For Windows Embedded devices with write filters, commit Endpoint Protection client installation (requires restart)**
   - **Allow Endpoint Protection client installation and restart to be performed outside maintenance windows**

     When the Configuration Manager client is installed, these settings install the Endpoint Protection client and ensure that it is persisted in the operating system as part of the installation, rather than written to the overlay only. The company security policies require that the antimalware software is always installed and the Admin does not want to run the risk of the kiosks being unprotected for even a short period of time if they restart.

   > **NOTE**
   > The restarts that are required to install the Endpoint Protection client are a one-time occurrence, which happen during the setup period for the devices and before the visitor center is operational. Unlike the periodic deployment of applications or software definition updates, the next time the Endpoint Protection client is installed on the same device will probably be when the company upgrades to the next version of Configuration Manager.

   For more information, see Configuring Endpoint Protection in System Center Configuration Manager.

6. With the configuration settings for the client now in place, the Admin prepares to install the Configuration Manager clients. Before the Admin can install the clients, they must manually disable the write filter on the Windows Embedded devices. The Admin reads the OEM documentation that accompanies the kiosks and follows their instructions to disable the write filters.

   The Admin renames the device so it uses the company standard naming format, and then installs the client manually by running CCMSetup with the following command from a mapped drive that holds the client source files: **CCMSetup.exe /MP:mpserver.cohovineyardandwinery.com SMSSITECODE=CO1**

   This command installs the client, assigns the client to the management point that has the intranet FQDN of **mpserver.cohovineyardandwinery.com**, and assigns the client to the primary site named **CO1**.

   The Admin knows that it always takes a while for clients to install and send back their status to the site. So the Admin waits before they confirm that the clients successfully install, assign to the site, and appear as clients in the collection that they created for Windows Embedded devices.

   As additional confirmation, the Admin checks the properties of Configuration Manager in Control Panel on the devices and compares them to standard Windows computers that are managed by the site. For example, on the **Components** tab, the **Hardware Inventory Agent** displays **Enabled**, and on the **Actions** tab, there are 11 available actions, which include **Application Deployment Evaluation Cycle** and **Discovery Data Collection Cycle**.

   Confident that the clients are successfully installed, assigned, and receiving client policy from the management point, the Admin then manually enables the write filters by following the instructions from the OEM.

   For more information, see:

   - How to deploy clients to Windows computers in System Center Configuration Manager
   - How to assign clients to a site in System Center Configuration Manager

7. Now that the Configuration Manager client is installed on the Windows Embedded devices, the Admin confirms that they can manage them in the same way as they manage the standard Windows clients. For example, from the Configuration Manager console, the Admin can remotely manage them by using remote control, initiate client policy for them, and view client properties and hardware inventory.

   Because these devices are joined to an Active Directory domain, the Admin does not have to manually approve them as trusted clients and confirms from the Configuration Manager console that they are approved.

   For more information, see How to manage clients in System Center Configuration Manager.

8. To install the interactive presentation software, the Admin runs the **Deploy Software Wizard** and configures a required application. On the **User Experience** page of the wizard, in the **Write filter handling for Windows Embedded devices** section, they accept the default option that selects **Commit changes at deadline or during a maintenance window (requires restarts)**.

   The Admin keeps this default option for write filters to ensure that the application persists after a restart, so that it is always available to the visitors using the kiosks. The daily maintenance window provides a safe period during which the restarts for installation and any updates can occur.

   The Admin deploys the application to the Windows Embedded devices collection.

   For more information, see How to deploy applications with System Center Configuration Manager.

9. To configure definition updates for Endpoint Protection, the Admin uses software updates and runs the Create Automatic Deployment Rule Wizard. They select the **Definition Updates** template to prepopulate the wizard with settings that are appropriate for Endpoint Protection.

   These settings include the following on the **User Experience** page of the wizard:

   - **Deadline behavior**: The **Software Installation** check box is not selected.
   - **Write filter handling for Windows Embedded devices**: The **Commit changes at deadline or during a maintenance window (requires restarts)** check box is not selected.

     The Admin keeps these default settings. Together, these two options with this configuration allow any software update definitions for Endpoint Protection to be installed in the overlay during the day and not wait to be installed and committed during the maintenance window. This configuration best meets the company security policy for computers to run up-to-date antimalware protection.

     > **NOTE**
     > Unlike software installations for applications, software update definitions for Endpoint Protection can occur very frequently, even multiple times a day. They are often small files. For these types of security-related deployments, it can often be beneficial to always install to the overlay rather than wait until the maintenance window. The Configuration Manager client will quickly re-install the software definition updates if the device restarts because this action initiates an evaluation check and does not wait until the next scheduled evaluation.

     The Admin selects the Windows Embedded devices collection for the automatic deployment rule.

     For more information, see
     Step 3: Configure Configuration Manager Software Updates to Deliver Definition Updates to Client Computers in Configuring Endpoint Protection in System Center Configuration Manager

10. The Admin decides to configure a maintenance task that periodically commits all changes on the overlay. This task is to support the software update definitions deployment, to reduce the number of updates that accumulate and must be installed again, each time the device restarts. In the Admin's experience, this helps

the antimalware programs run more efficiently.

> **NOTE**
> These software update definitions would be automatically committed to the image if the embedded devices ran another management task that supported committing the changes. For example, installing a new version of the interactive presentation software would also commit the changes for software update definitions. Or, installing standard software updates every month that install during the maintenance window could also commit the changes for software update definitions. However, in this scenario, where standard software updates do not run and the interactive presentation software is unlikely to be updated very often, it might be months before the software definition updates are automatically committed to the image.

The Admin first creates a custom task sequence that has no settings other than the name. They run the Create Task Sequence Wizard:

a. On the **Create a New Task Sequence** page, the Admin selects **Create a new custom task sequence**, and then clicks **Next**.

b. On the **Task Sequence Information** page, the Admin enters **Maintenance task to commit changes on embedded devices** for the task sequence name, and then clicks **Next**.

c. On the **Summary** page, the Admin selects **Next**, and completes the wizard.

   The Admin then deploys this custom task sequence to the Windows Embedded devices collection, and configures the schedule to run every month. As part of the deployment settings, they select the **Commit changes at deadline or during a maintenance window (requires restarts)** check box to persist the changes after a restart. To configure this deployment, the Admin selects the custom task sequence that they just created, and then on the **Home** tab, in the **Deployment** group, they click **Deploy** to start the Deploy Software Wizard:

d. On the **General** page, the Admin selects the Windows Embedded devices collection, and then clicks **Next**.

e. On the **Deployment Settings** page, the Admin selects the **Purpose** of **Required**, and then clicks **Next**.

f. On the **Scheduling** page, the Admin clicks **New** to specify a weekly schedule during the maintenance window, and then clicks **Next**.

g. The Admin completes the wizard without any further changes.

   For more information, see
   Manage task sequences to automate tasks in System Center Configuration Manager.

11. For the kiosks to run automatically, the Admin writes a script to configure the devices for the following settings:

    - Automatically log on, using a guest account that has no password.
    - Automatically run the interactive presentation software on startup.

    The Admin uses packages and programs to deploy this script to the Windows Embedded devices collection. When the Admin runs the Deploy Software Wizard, they again select the **Commit changes at deadline or during a maintenance window (requires restarts)** check box to persist the changes after a restart.

    For more information, see Packages and programs in System Center Configuration Manager.

12. The following morning, the Admin checks the Windows Embedded devices. They confirm the following:

- The kiosk is automatically logged on by using the guest account.
- The interactive presentation software is running.
- The Endpoint Protection client is installed and has the latest software update definitions.
- That the device restarted during the maintenance window.

  For more information, see:

- How to monitor Endpoint Protection in System Center Configuration Manager
- Monitor applications with System Center Configuration Manager

13. The Admin monitors the kiosks and reports the successful management of them to their manager. As a result, 20 kiosks are ordered for the visitor center.

    To avoid the manual installation of the Configuration Manager client, which requires manually disabling and then enabling the write filters, the Admin ensures that the order includes a customized image that already includes the installation and site assignment of the Configuration Manager client. In addition, the devices are named according to the company naming format.

    The kiosks are delivered to the visitor center a week before it opens. During this time, the kiosks are connected to the network, all device management for them is automatic, and no local administrator is required. The Admin confirms that the kiosks are functioning as required:

    - The clients on the kiosks complete site assignment and download the trusted root key from Active Directory Domain Services.
    - The clients on the kiosks are automatically added to the Windows Embedded devices collection and configured with the maintenance window.
    - The Endpoint Protection client is installed and has the latest software update definitions for antimalware protection.
    - The interactive presentation software is installed and runs automatically, ready for visitors.

14. After this initial setup, any restarts that might be required for updates occur only when the visitor center is closed.

Plan how to wake up clients in System Center Configuration Manager

4/23/2019 • 7 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Configuration Manager supports traditional wake-up packets to wake up computers in sleep mode when you want to install required software, such as software updates and applications.

> **NOTE**
> This article describes how an older version of Wake on LAN functions. This functionality still exists in Configuration Manager version 1810, which also includes a newer version of Wake on LAN too. Both versions of Wake on LAN can, and in many cases will, be enabled simultaneously. For more information about how the new version of Wake on LAN functions starting in 1810 and enabling either or both versions, see How to configure Wake on LAN.

How to wake up clients in System Center Configuration Manager

Configuration Manager supports traditional wake-up packets to wake up computers in sleep mode when you want to install required software, such as software updates and applications.

You can supplement the traditional wake-up packet method by using the wake-up proxy client settings. Wake-up proxy uses a peer-to-peer protocol and elected computers to check whether other computers on the subnet are awake, and to wake them if necessary. When the site is configured for Wake On LAN and clients are configured for wake-up proxy, the process works as follows:

1. Computers with the Configuration Manager client installed and that aren't asleep on the subnet check whether other computers on the subnet are awake. They do this check by sending each other a TCP/IP ping command every five seconds.

2. If there's no response from other computers, they're assumed to be asleep. The computers that are awake become *manager computer* for the subnet.

   Because it's possible that a computer might not respond because of a reason other than it's asleep (for example, it's turned off, removed from the network, or the proxy wake-up client setting is no longer applied), the computers are sent a wake-up packet every day at 2 P.M. local time. Computers that don't respond will no longer be assumed to be asleep and will not be woken up by wake-up proxy.

   To support wake-up proxy, at least three computers must be awake for each subnet. To achieve this requirement, three computers are non-deterministically chosen to be *guardian computers* for the subnet. This state means that they stay awake, despite any configured power policy to sleep or hibernate after a period of inactivity. Guardian computers honor shutdown or restart commands, for example, as a result of maintenance tasks. If this action happens, the remaining guardian computers wake up another computer on the subnet so that the subnet continues to have three guardian computers.

3. Manager computers ask the network switch to redirect network traffic for the sleeping computers to themselves.

   The redirection is achieved by the manager computer broadcasting an Ethernet frame that uses the sleeping computer's MAC address as the source address. This behavior makes the network switch behave as if the sleeping computer has moved to the same port that the manager computer is on. The manager computer

also sends ARP packets for the sleeping computers to keep the entry fresh in the ARP cache. The manager computer also responds to ARP requests on behalf of the sleeping computer and replies with the MAC address of the sleeping computer.

> **WARNING**
> During this process, the IP-to-MAC mapping for the sleeping computer remains the same. Wake-up proxy works by informing the network switch that a different network adapter is using the port that was registered by another network adapter. However, this behavior is known as a MAC flap and is unusual for standard network operation. Some network monitoring tools look for this behavior and can assume that something is wrong. Consequently, these monitoring tools can generate alerts or shut down ports when you use wake-up proxy.
>
> Do not use wake-up proxy if your network monitoring tools and services do not allow MAC flaps.

4. When a manager computer sees a new TCP connection request for a sleeping computer and the request is to a port that the sleeping computer was listening on before it went to sleep, the manager computer sends a wake-up packet to the sleeping computer, and then stops redirecting traffic for this computer.
5. The sleeping computer receives the wake-up packet and wakes up. The sending computer automatically retries the connection and this time, the computer is awake and can respond.

Wake-up proxy has the following prerequisites and limitations:

> **IMPORTANT**
> If you have a separate team that is responsible for the network infrastructure and network services, notify and include this team during your evaluation and testing period. For example, on a network that uses 802.1X network access control, wake-up proxy will not work and can disrupt the network service. In addition, wake-up proxy could cause some network monitoring tools to generate alerts when the tools detect the traffic to wake-up other computers.

- All Windows operating systems listed as supported clients in Supported operating systems for clients and devices are supported for Wake On LAN.
- Guest operating systems that run on a virtual machine are not supported.
- Clients must be enabled for wake-up proxy by using client settings. Although wake-up proxy operation does not depend on hardware inventory, clients do not report the installation of the wake-up proxy service unless they are enabled for hardware inventory and submitted at least one hardware inventory.
- Network adapters (and possibly the BIOS) must be enabled and configured for wake-up packets. If the network adapter is not configured for wake-up packets or this setting is disabled, Configuration Manager will automatically configure and enable it for a computer when it receives the client setting to enable wake-up proxy.
- If a computer has more than one network adapter, you cannot configure which adapter to use for wake-up proxy; the choice is non-deterministic. However, the adapter chosen is recorded in the SleepAgent_<DOMAIN>@SYSTEM_0.log file.
- The network must allow ICMP echo requests (at least within the subnet). You cannot configure the five-second interval that is used to send the ICMP ping commands.
- Communication is unencrypted and unauthenticated, and IPsec is not supported.
- The following network configurations are not supported:
  - 802.1X with port authentication
  - Wireless networks

- Network switches that bind MAC addresses to specific ports
- IPv6-only networks
- DHCP lease durations less than 24 hours

If you want to wake up computers for scheduled software installation, you must configure each primary site to use wake-up packets.

To use wake-up proxy, you must deploy Power Management wake-up proxy client settings in addition to configuring the primary site.

Decide whether to use subnet-directed broadcast packets, or unicast packets, and what UDP port number to use. By default, traditional wake-up packets are transmitted by using UDP port 9, but to help increase security, you can select an alternative port for the site if this alternative port is supported by intervening routers and firewalls.

Choose Between Unicast and Subnet-Directed Broadcast for Wake-on-LAN

If you chose to wake up computers by sending traditional wake-up packets, you must decide whether to transmit unicast packets or subnet-direct broadcast packets. If you use wake-up proxy, you must use unicast packets. Otherwise, use the following table to help you determine which transmission method to choose.

TRANSMISSION METHOD	ADVANTAGE	DISADVANTAGE
Unicast	More secure solution than subnet-directed broadcasts because the packet is sent directly to a computer instead of to all computers on a subnet. Might not require reconfiguration of routers (you might have to configure the ARP cache). Consumes less network bandwidth than subnet-directed broadcast transmissions. Supported with IPv4 and IPv6.	Wake-up packets do not find destination computers that have changed their subnet address after the last hardware inventory schedule. Switches might have to be configured to forward UDP packets. Some network adapters might not respond to wake-up packets in all sleep states when they use unicast as the transmission method.

TRANSMISSION METHOD	ADVANTAGE	DISADVANTAGE
Subnet-Directed Broadcast	Higher success rate than unicast if you have computers that frequently change their IP address in the same subnet. No switch reconfiguration is required. High compatibility rate with computer adapters for all sleep states, because subnet-directed broadcasts were the original transmission method for sending wake-up packets.	Less secure solution than using unicast because an attacker could send continuous streams of ICMP echo requests from a falsified source address to the directed broadcast address. This causes all of the hosts to reply to that source address. If routers are configured to allow subnet-directed broadcasts, the additional configuration is recommended for security reasons: - Configure routers to allow only IP-directed broadcasts from the Configuration Manager site server, by using a specified UDP port number. - Configure Configuration Manager to use the specified non-default port number. Might require reconfiguration of all intervening routers to enable subnet-directed broadcasts. Consumes more network bandwidth than unicast transmissions. Supported with IPv4 only; IPv6 is not supported.

WARNING

There are security risks associated with subnet-directed broadcasts: An attacker could send continuous streams of Internet Control Message Protocol (ICMP) echo requests from a falsified source address to the directed broadcast address, which cause all the hosts to reply to that source address. This type of denial of service attack is commonly called a smurf attack and is typically mitigated by not enabling subnet-directed broadcasts.

Manage Configuration Manager clients in a virtual desktop infrastructure (VDI)

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

System Center Configuration Manager supports installing the Configuration Manager client on the following virtual desktop infrastructure (VDI) scenarios:

- **Personal virtual machines** - Personal virtual machines are generally used when you want to make sure that user data and settings are maintained on the virtual machine between sessions.
- **Remote Desktop Services sessions** - Remote Desktop Services enables a server to host multiple, concurrent client sessions. Users can connect to a session and then run applications on that server.
- **Pooled virtual machines** - Pooled virtual machines are not persisted between sessions. When a session is closed, all data and settings are discarded. Pooled virtual machines are useful when Remote Desktop Services cannot be used because a required business application cannot run on the Windows Server that hosts the client sessions.

  The following table lists considerations for managing the Configuration Manager client in a virtual desktop infrastructure.

VIRTUAL MACHINE TYPE	CONSIDERATIONS
Personal virtual machines	Configuration Manager treats personal virtual machines identically to a physical computer. The Configuration Manager client can be preinstalled on the virtual machine image or deployed after the virtual machine is provisioned.
Remote Desktop Services	The Configuration Manager client is not installed for individual Remote Desktop sessions. Instead, the client is only installed one time on the Remote Desktop Services server. All Configuration Manager features can be used on the Remote Desktop Services server.
Pooled virtual machines	When a pooled virtual machine is decommissioned, any changes that you make by using Configuration Manager are lost. Data returned from Configuration Manager features such as hardware inventory, software inventory and software metering might not be relevant to your needs as the virtual machine might only be operational for a short length of time. Consider excluding pooled virtual machines from inventory tasks.

Because virtualization supports running multiple Configuration Manager clients on the same physical computer, many client operations have a built-in randomized delay for scheduled actions such as hardware and software inventory, antimalware scans, software installations, and software update scans. This delay helps distribute the CPU processing and data transfer for a computer that has multiple virtual machines that run the Configuration Manager client.

NOTE

With the exception of Windows Embedded clients that are in servicing mode, Configuration Manager clients that are not running in virtualized environments also use this randomized delay. When you have many deployed clients, this behavior helps avoid peaks in network bandwidth and reduces the CPU processing requirement on the Configuration Manager site systems, such as the management point and site server. The delay interval varies according to the Configuration Manager capability.

The randomization delay is disabled by default for required software updates by using the following client setting: **Computer Agent**: **Disable deadline randomization**.

How to configure client communication ports in System Center Configuration Manager

2/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can change the request port numbers that System Center Configuration Manager clients use to communicate with site systems that use HTTP and HTTPS for communication. Although HTTP or HTTPS is more likely to be already configured for firewalls, client notification that uses HTTP or HTTPS requires more CPU usage and memory on the management point computer than if you use a custom port number. You can also specify the site port number to use if you wake up clients by using traditional wake-up packets.

When you specify HTTP and HTTPS request ports, you can specify both a default port number and an alternative port number. Clients automatically try the alternative port after communication fails with the default port. You can specify settings for HTTP and HTTPS data communication.

The default values for client request ports are **80** for HTTP traffic and **443** for HTTPS traffic. Change them only if you do not want to use these default values. A typical scenario for using custom ports is when you use a custom website in IIS rather than the default website. If you change the default port numbers for the default website in IIS and other applications also use the default website, they are likely to fail.

> **IMPORTANT**
> Do not change the port numbers in Configuration Manager without understanding the consequences. Examples:
>
> - If you change the port numbers for the client request services as a site configuration and existing clients are not reconfigured to use the new port numbers, these clients will become unmanaged.
>   - Before you configure a non-default port number, make sure that firewalls and all intervening network devices can support this configuration and reconfigure them as necessary. If you will manage clients on the Internet and change the default HTTPS port number of 443, routers and firewalls on the Internet might block this communication.

To make sure that clients do not become unmanaged after you change the request port numbers, clients must be configured to use the new request port numbers. When you change the request ports on a primary site, any attached secondary sites automatically inherit the same port configuration. Use the procedure in this topic to configure the request ports on the primary site.

> **NOTE**
> For information about how to configure the request ports for clients on computers that run Linux and UNIX, see Configure Request Ports for the Client for Linux and UNIX.

When the Configuration Manager site is published to Active Directory Domain Services, new and existing clients that can access this information will automatically be configured with their site port settings and you do not need to take further action. Clients that cannot access this information published to Active Directory Domain Services include workgroup clients, clients from another Active Directory forest, clients that are configured for Internet-only, and clients that are currently on the Internet. If you change the default port numbers after these clients have been installed, reinstall them and install any new clients by using one of the following methods:

- Reinstall the clients by using the Client Push Installation Wizard. Client push installation automatically

configures clients with the current site port configuration. For more information about how to use the Client Push Installation Wizard, see How to Install Configuration Manager Clients by Using Client Push.

- Reinstall the clients by using CCMSetup.exe and the client.msi installation properties of CCMHTTPPORT and CCMHTTPSPORT. For more information about these properties, see About client installation properties in System Center Configuration Manager.
- Reinstall the clients by using a method that searches Active Directory Domain Services for Configuration Manager client installation properties. For more information, see About client installation properties published to Active Directory Domain Services in System Center Configuration Manager.

  To reconfigure the port numbers for existing clients, you can also use the script PORTSWITCH.VBS that is provided with the installation media in the SMSSETUP\Tools\PortConfiguration folder.

> **IMPORTANT**
> For existing and new clients that are currently on the Internet, you must configure the non-default port numbers by using the CCMSetup.exe client.msi properties of CCMHTTPPORT and CCMHTTPSPORT.

After changing the request ports on the site, new clients that are installed by using the site-wide client push installation method will be automatically configured with the current port numbers for the site.

To configure the client communication port numbers for a site

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Site Configuration**, click **Sites**, and select the primary site to configure.
3. On the **Home** tab, click **Properties**, and then click the **Ports** tab.
4. Select any of the items and click the Properties icon to display the **Port Detail** dialog box.
5. In the **Port Detail** dialog box, specify the port number and description for the item, and then click **OK**.
6. Select **Use custom web site** if you will use the custom website name of **SMSWeb** for site systems that run IIS.
7. Click **OK** to close the properties dialog box for the site.

   Repeat this procedure for all primary sites in the hierarchy.

Configure client computers to find management points by using DNS publishing

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Clients in System Center Configuration Manager must locate a management point to complete site assignment and as an on-going process to remain managed. Active Directory Domain Services provides the most secure method for clients on the intranet to find management points. However, if clients cannot use this service location method (for example, you have not extended the Active Directory schema, or clients are from a workgroup), use DNS publishing as the preferred alternative service location method.

> **NOTE**
> When you install the client for Linux and UNIX, you must specify a management point to use as an initial point of contact. For information about how to install the client for Linux and UNIX, see How to deploy clients to UNIX and Linux servers in System Center Configuration Manager.

Before you use DNS publishing for management points, make sure that DNS servers on the intranet have service location resource records (SRV RR) and corresponding host (A or AAA) resource records for the site's management points. The service location resource records can be created automatically by Configuration Manager or manually, by the DNS administrator who creates the records in DNS.

For more information about DNS publishing as a service location method for Configuration Manager clients, see Understand how clients find site resources and services for System Center Configuration Manager.

By default, clients search DNS for management points in their DNS domain. However, if there are no management points published in the clients' domain, you must manually configure clients with a management point DNS suffix. You can configure this DNS suffix on clients either during or after client installation:

- To configure clients for a management point suffix during client installation, configure the CCMSetup Client.msi properties.
- To configure clients for a management point suffix after client installation, in Control Panel, configure the **Configuration Manager Properties**.

To configure clients for a management point suffix during client installation

- Install the client with the following CCMSetup Client.msi property:
  - **DNSSUFFIX=** *<management point domain>*

    If the site has more than one management point and they are in more than one domain, specify just one domain. When clients connect to a management point in this domain, they download a list of available management points, which will include the management points from the other domains.

    For more information about the CCMSetup command-line properties, see About client installation properties in System Center Configuration Manager.

To configure clients for a management point suffix after client installation

1. In Control Panel of the client computer, navigate to **Configuration Manager**, and then double-click **Properties**.
2. On the **Site** tab, specify the DNS suffix of a management point, and then click **OK**.

If the site has more than one management point and they are in more than one domain, specify just one domain. When clients connect to a management point in this domain, they download a list of available management points, which will include the management points from the other domains.

How to configure client settings in System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You manage all client settings in System Center Configuration Manager from **Administration** > **Client Settings**. Modify the default settings when you want to configure settings for all users and devices in the hierarchy that do not have any custom settings applied. If you want to apply different settings to just some users or devices, create custom settings and deploy to collections.

For information about each client setting, see About client settings in System Center Configuration Manager.

> **NOTE**
> You can also use configuration items to manage clients to assess, track, and remediate the configuration compliance of devices. For more information, see Ensure device compliance with System Center Configuration Manager.

Configure the default client settings

1. In the Configuration Manager console, choose **Administration** > **Client Settings** > **Default Client Settings**.
2. On the **Home** tab, choose **Properties**.
3. View and configure the client settings for each group of settings in the navigation pane.

   Client computers will be configured with these settings when they next download client policy. To initiate policy retrieval for a single client, see Initiate Policy Retrieval for a Configuration Manager Client in How to manage clients in System Center Configuration Manager.

Create and deploy custom client settings

When you deploy these custom settings, they override the default client settings. Before you begin this procedure, ensure that you have a collection that contains the users or devices that require these custom client settings.

1. In the Configuration Manager console, choose **Administration** > **Client Settings**.
2. On the **Home** tab, in the **Create** group, choose **Create Custom Client Settings**, and then choose either:
   - **Create Custom Client Device Settings**
   - **Create Custom Client User Settings**
3. Specify a unique name and option description.
4. Select one or more of the check boxes that display a group of settings.
5. Choose each group of settings from the navigation pane, and configure the available settings, then click **OK**.
6. Select the custom client setting that you created. On the **Home** tab, in the **Client Settings** group, choose **Deploy**.

7. In the **Select Collection** dialog box, select the appropriate collection, and then choose **OK**. You can verify the selected collection if you click the **Deployments** tab in the details pane.

8. View the order of the custom client setting that you created. When you have multiple custom client settings, they are applied according to their order number. If there are any conflicts, the setting that has the lowest order number overrides the other settings. To change the order number, on the **Home** tab, in the **Client Settings** group, choose **Move Item Up** or **Move Item Down**.

   Client computers will be configured with these settings when they next download client policy. To initiate policy retrieval for a single client, see Initiate Policy Retrieval for a Configuration Manager Client in How to manage clients in System Center Configuration Manager.

View client settings

When you deploy multiple client settings to the same device, user, or user group, the prioritization and combination of settings is complex. To view the client settings:

1. In the Configuration Manager console, choose **Assets and Compliance** > **Devices** > **Users** or **User Collections**.

2. Select a device, user, or user group and in the **Client Settings** group, select **Resultant Client Settings**.

3. Select a client setting from the left pane, and the settings are displayed. In this view, the settings are read-only.

   > **NOTE**
   > To view the client settings, you must have read access to Client Settings.

About client settings in Configuration Manager

8/23/2019 • 40 minutes to read • Edit Online

Applies to: System Center Configuration Manager (current branch)

Manage all client settings in the Configuration Manager console from the **Client Settings** node in the **Administration** workspace. Configuration Manager comes with a set of default settings. When you change the default client settings, these settings are applied to all clients in the hierarchy. You can also configure custom client settings, which override the default client settings when you assign them to collections. For more information, see How to configure client settings.

The following sections describe settings and options in further detail.

Background Intelligent Transfer Service (BITS)

Limit the maximum network bandwidth for BITS background transfers

When this option is **Yes**, clients use BITS bandwidth throttling. To configure the other settings in this group, you must enable this setting.

Throttling window start time

Specify the local start time for the BITS throttling window.

Throttling window end time

Specify the local end time for the BITS throttling window. If the end time is equal to the **Throttling window start time**, BITS throttling is always enabled.

Maximum transfer rate during throttling window (Kbps)

Specify the maximum transfer rate that clients can use during the window.

Allow BITS downloads outside the throttling window

Allow clients to use separate BITS settings outside the specified window.

Maximum transfer rate outside the throttling window (Kbps)

Specify the maximum transfer rate that clients can use outside the BITS throttling window.

Client cache settings

Configure BranchCache

Set up the client computer for Windows BranchCache. To allow BranchCache caching on the client, set **Enable BranchCache** to **Yes**.

- **Enable BranchCache**: Enables BranchCache on client computers.
- **Maximum BranchCache cache size (percentage of disk)**: The percentage of the disk that you allow BranchCache to use.

Configure client cache size

The Configuration Manager client cache on Windows computers stores temporary files used to install applications and programs. If this option is set to **No**, the default size is 5,120 MB.

If you choose **Yes**, then specify:

- **Maximum cache size (MB)**
- **Maximum cache size (percentage of disk)**: The client cache size expands to the maximum size in megabytes (MB), or the percentage of the disk, whichever is less.

Enable as peer cache source

> **NOTE**
> In version 1902 and earlier, this setting was named **Enable Configuration Manager client in full OS to share content**. The behavior of the setting didn't change.

Enables peer cache for Configuration Manager clients. Choose **Yes**, and then specify the port through which the client communicates with the peer computer.

- **Port for initial network broadcast** (default UDP 8004): Configuration Manager uses this port in Windows PE or the full Windows OS. The task sequence engine in Windows PE sends the broadcast to get content locations before it starts the task sequence.
- **Port for content download from peer** (default TCP 8003): Configuration Manager automatically configures Windows Firewall rules to allow this traffic. If you use a different firewall, you must manually configure rules to allow this traffic.

  For more information, see Ports used for connections.

Minimum duration before cached content can be removed (minutes)

Starting in version 1906, specify the minimum time for the Configuration Manager client to keep cached content. This client setting defines the minimum amount of time Configuration Manager agent should wait before it can remove content from the cache in case more space is needed.

By default this value is 1,440 minutes (24 hours). The maximum value for this setting is 10,080 minutes (1 week).

This setting gives you greater control over the client cache on different types of devices. You might reduce the value on clients that have small hard drives and don't need to keep existing content before another deployment runs.

Client policy

Client policy polling interval (minutes)

Specifies how frequently the following Configuration Manager clients download client policy:

- Windows computers (for example, desktops, servers, laptops)
- Mobile devices that Configuration Manager enrolls
- Mac computers
- Computers that run Linux or UNIX

This value is 60 minutes by default. Reducing this value causes clients to poll the site more frequently. With numerous clients, this behavior can have a negative impact on the site performance. The size and scale guidance is based on the default value. Increasing this value causes clients to poll the site less often. Any changes to client policies, including new deployments, take longer for clients to download and process.

Enable user policy on clients

When you set this option to **Yes**, and use user discovery, then clients receive applications and programs targeted to the signed-in user.

If this setting is **No**, users don't receive required applications that you deploy to users. Users also don't receive any other management tasks in user policies.

This setting applies to users when their computer is on either the intranet or the internet. It must be **Yes** if you also want to enable user policies on the internet.

> **NOTE**
>
> Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You can't install new application catalog roles.
>
> If you're still using the application catalog, it receives the list of available software for users from the site server. Thus, this setting doesn't have to be **Yes** for users to see and request applications from the application catalog. If this setting is **No**, users can't install the applications that they see in the application catalog.

Enable user policy requests from internet clients

Set this option to **Yes** for users to receive the user policy on internet-based computers. The following requirements also apply:

- The client and site are configured for internet-based client management or a cloud management gateway.
- The **Enable user policy on clients** setting is **Yes**.
- The internet-based management point successfully authenticates the user by using Windows authentication (Kerberos or NTLM). For more information, see Considerations for client communications from the internet.
- The cloud management gateway successfully authenticates the user by using Azure Active Directory. For more information, see Deploy user-available applications on Azure AD-joined devices.

If you set this option to **No**, or any of the previous requirements aren't met, then a computer on the internet only receives computer policies. In this scenario, users can still see, request, and install applications from an internet-based application catalog. If this setting is **No**, but **Enable user policy on clients** is **Yes**, users don't receive user policies until the computer is connected to the intranet.

> **NOTE**
>
> For internet-based client management, application approval requests from users don't require user policies or user authentication. The cloud management gateway doesn't support application approval requests.

Cloud services

Allow access to cloud distribution point

Set this option to **Yes** for clients to obtain content from a cloud distribution point. This setting doesn't require the device to be internet-based.

Automatically register new Windows 10 domain joined devices with Azure Active Directory

When you configure Azure Active Directory to support hybrid join, Configuration Manager configures Windows 10 devices for this functionality. For more information, see How to configure hybrid Azure Active Directory joined devices.

Enable clients to use a cloud management gateway

By default, all internet-roaming clients use any available cloud management gateway. An example of when to configure this setting to **No** is to scope usage of the service, such as during a pilot project or to save costs.

Compliance settings

Enable compliance evaluation on clients

Set this option to **Yes** to configure the other settings in this group.

Schedule compliance evaluation

Select **Schedule** to create the default schedule for configuration baseline deployments. This value is configurable for each baseline in the **Deploy Configuration Baseline** dialog box.

Enable User Data and Profiles

Choose **Yes** if you want to deploy user data and profiles configuration items.

Computer agent

User notifications for required deployments

For more information about the following three settings, see User notifications for required deployments:

- **Deployment deadline greater than 24 hours, remind user every (hours)**
- **Deployment deadline less than 24 hours, remind user every (hours)**
- **Deployment deadline less than 1 hour, remind user every (minutes)**

Default Application Catalog website point

> **IMPORTANT**
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features

Configuration Manager uses this setting to connect users to the application catalog from Software Center. Select **Set Website** to specify a server that hosts the application catalog website point. Enter its NetBIOS name or FQDN, specify automatic detection, or specify a URL for customized deployments. In most cases, automatic detection is the best choice.

Add default Application Catalog website to Internet Explorer trusted sites zone

> **IMPORTANT**
> The application catalog's Silverlight user experience isn't supported as of current branch version 1806. Starting in version 1906, updated clients automatically use the management point for user-available application deployments. You also can't install new application catalog roles. In the first current branch release after October 31, 2019, support will end for the application catalog roles.
>
> For more information, see the following articles:
>
> - Configure Software Center
> - Removed and deprecated features

If this option is **Yes**, the client automatically adds the current default application catalog website URL to the Internet Explorer trusted sites zone.

This setting ensures that the Internet Explorer setting for Protected Mode isn't enabled. If Protected Mode is enabled, the Configuration Manager client might not be able to install applications from the application catalog. By default, the trusted sites zone also supports user sign-in for the application catalog, which requires Windows

authentication.

If you leave this option as **No**, Configuration Manager clients might not be able to install applications from the application catalog. An alternative method is to configure these Internet Explorer settings in another zone for the application catalog URL that clients use.

Allow Silverlight applications to run in elevated trust mode

> **IMPORTANT**
> The client doesn't automatically install Silverlight.
>
> Starting in version 1806, the **Silverlight user experience** for the application catalog website point is no longer supported. Users should use the new Software Center. For more information, see Configure Software Center.

This setting must be **Yes** for users to use the application catalog.

If you change this setting, it takes effect when users next load their browser, or refresh their currently opened browser window.

For more information about this setting, see Certificates for Microsoft Silverlight 5, and elevated trust mode required for the application catalog.

Organization name displayed in Software Center

Type the name that users see in Software Center. This branding information helps users to identify this application as a trusted source. For more information about the priority of this setting, see Branding Software Center.

Use new Software Center

The default setting is **Yes**.

When you set this option to **Yes**, then all client computers use the Software Center. Software Center shows software, software updates, and task sequences that you deploy to users or devices.

Enable communication with Health Attestation Service

Set this option to **Yes** for Windows 10 devices to use Health attestation. When you enable this setting, the following setting is also available for configuration.

Use on-premises Health Attestation Service

Set this option to **Yes** for devices to use an on-premises service. Set to **No** for devices to use the Microsoft cloud-based service.

Install permissions

Configure how users can install software, software updates, and task sequences:

- **All Users**: Users with any permission except Guest.
- **Only Administrators**: Users must be a member of the local Administrators group.
- **Only Administrators and primary users**: Users must be a member of the local Administrators group, or a primary user of the computer.
- **No Users**: No users signed in to a client computer can install software, software updates, and task sequences. Required deployments for the computer always install at the deadline. Users can't install software from Software Center.

Suspend BitLocker PIN entry on restart

If computers require BitLocker PIN entry, then this option bypasses the requirement to enter a PIN when the computer restarts after a software installation.

- **Always**: Configuration Manager temporarily suspends BitLocker after it has installed software that requires a restart, and has initiated a restart of the computer. This setting applies only to a computer restart initiated by Configuration Manager. This setting doesn't suspend the requirement to enter the BitLocker PIN when the user restarts the computer. The BitLocker PIN entry requirement resumes after Windows startup.
- **Never**: Configuration Manager doesn't suspend BitLocker after it has installed software that requires a restart. In this scenario, the software installation can't finish until the user enters the PIN to complete the standard startup process and load Windows.

Additional software manages the deployment of applications and software updates

Enable this option only if one of the following conditions applies:

- You use a vendor solution that requires this setting to be enabled.
- You use the Configuration Manager software development kit (SDK) to manage client agent notifications, and the installation of applications and software updates.

> **WARNING**
> If you choose this option when neither of these conditions apply, the client doesn't install software updates and required applications. This setting doesn't prevent users from installing available software from Software Center, including applications, packages, and task sequences.

PowerShell execution policy

Configure how Configuration Manager clients can run Windows PowerShell scripts. You might use these scripts for detection in configuration items for compliance settings. You might also send the scripts in a deployment as a standard script.

- **Bypass**: The Configuration Manager client bypasses the Windows PowerShell configuration on the client computer, so that unsigned scripts can run.
- **Restricted**: The Configuration Manager client uses the current PowerShell configuration on the client computer. This configuration determines whether unsigned scripts can run.
- **All Signed**: The Configuration Manager client runs scripts only if a trusted publisher has signed them. This restriction applies independently from the current PowerShell configuration on the client computer.

This option requires at least Windows PowerShell version 2.0. The default is **All Signed**.

> **TIP**
> If unsigned scripts fail to run because of this client setting, Configuration Manager reports this error in the following ways:
>
> - The **Monitoring** workspace in the console displays deployment status error ID **0x87D00327**. It also displays the description **Script is not signed**.
> - Reports display the error type **Discovery Error**. Then reports display either error code **0x87D00327** and the description **Script is not signed**, or error code **0x87D00320** and the description **The script host has not been installed yet**. An example report is: **Details of errors of configuration items in a configuration baseline for an asset**.
> - The **DcmWmiProvider.log** file displays the message **Script is not signed (Error: 87D00327; Source: CCM)**.

Show notifications for new deployments

Choose **Yes** to display a notification for deployments available for less than a week. This message appears each time the client agent starts.

Disable deadline randomization

After the deployment deadline, this setting determines whether the client uses an activation delay of up to two

hours to install required software updates. By default, the activation delay is disabled.

For virtual desktop infrastructure (VDI) scenarios, this delay helps distribute the CPU processing and data transfer for a host machine with multiple virtual machines. Even if you don't use VDI, having many clients installing the same updates at the same time can negatively increase CPU usage on the site server. This behavior can also slow down distribution points, and significantly reduce the available network bandwidth.

If clients must install required software updates at the deployment deadline without delay, then configure this setting to **Yes**.

Grace period for enforcement after deployment deadline (hours)

If you want to give users more time to install required application or software update deployments beyond the deadline, set this option to **Yes**. This grace period is for a computer turned off for an extended time, and the user needs to install many application or update deployments. For example, this setting is helpful if a user returns from vacation, and has to wait for a long time while the client installs overdue application deployments.

Set a grace period of 1 to 120 hours. Use this setting along with the deployment property **Delay enforcement of this deployment according to user preferences**. For more information, see Deploy applications.

Computer restart

The following settings must be shorter in duration than the shortest maintenance window applied to the computer:

- **Display a temporary notification to the user that indicates the interval before the user is logged off or the computer restarts (minutes)**
- **Display a dialog box that the user cannot close, which displays the countdown interval before the user is logged off or the computer restarts (minutes)**

For more information about maintenance windows, see How to use maintenance windows.

- **Specify the snooze duration for computer restart countdown notifications (minutes)** (Starting in version 1906)
  - The default value is 240 minutes.
  - Your snooze duration value should be less than the temporary notification value minus the value for the notification the user cant dismiss.
  - For more information, see Device restart notifications.

When a deployment requires a restart, show a dialog window to the user instead of a toast notification: Starting in version 1902, configuring this setting to **Yes** changes the user experience to be more intrusive. This setting applies to all deployments of applications, task sequences, and software updates. For more information, see Plan for Software Center.

> **IMPORTANT**
> In Configuration Manager 1902, under certain circumstances, the dialog box won't replace toast notifications. To resolve this issue, install the update rollup for Configuration Manager version 1902.

Delivery Optimization

You use Configuration Manager boundary groups to define and regulate content distribution across your corporate network and to remote offices. Windows Delivery Optimization is a cloud-based, peer-to-peer technology to share content between Windows 10 devices. Configure Delivery Optimization to use your boundary groups when sharing content among peers.

> **NOTE**
> Delivery Optimization is only available on Windows 10 clients

Use Configuration Manager Boundary Groups for Delivery Optimization Group ID

Choose **Yes** to apply the boundary group identifier as the Delivery Optimization group identifier on the client. When the client communicates with the Delivery Optimization cloud service, it uses this identifier to locate peers with the desired content.

Enable devices managed by Configuration Manager to use Delivery Optimization In-Network Cache servers (Beta) for content download

Choose **Yes** to allow clients to download content from an on-premises distribution point that you enable as a Delivery Optimization In-Network Cache (DOINC) server. For more information, see Delivery Optimization In-Network Cache in Configuration Manager.

Endpoint Protection

> **TIP**
> In addition to the following information, you can find details about using Endpoint Protection client settings in Example scenario: Using Endpoint Protection to protect computers from malware.

Manage Endpoint Protection client on client computers

Choose **Yes** if you want to manage existing Endpoint Protection and Windows Defender clients on computers in your hierarchy.

Choose this option if you've already installed the Endpoint Protection client, and want to manage it with Configuration Manager. This separate installation includes a scripted process that uses a Configuration Manager application or package and program. Windows 10 devices don't need to have the Endpoint Protection agent installed. However, those devices will still need **Manage Endpoint Protection client on client computers** enabled.

Install Endpoint Protection client on client computers

Choose **Yes** to install and enable the Endpoint Protection client on client computers that aren't already running the client. Windows 10 clients don't need to have the Endpoint Protection agent installed.

> **NOTE**
> If the Endpoint Protection client is already installed, choosing **No** doesn't uninstall the Endpoint Protection client. To uninstall the Endpoint Protection client, set the **Manage Endpoint Protection client on client computers** client setting to **No**. Then, deploy a package and program to uninstall the Endpoint Protection client.

Allow Endpoint Protection client installation and restarts outside maintenance windows. Maintenance windows must be at least 30 minutes long for client installation

Set this option to **Yes** to override typical installation behaviors with maintenance windows. This setting meets business requirements for the priority of system maintenance for security purposes.

For Windows Embedded devices with write filters, commit Endpoint Protection client installation (requires restarts)

Choose **Yes** to disable the write filter on the Windows Embedded device, and restart the device. This action commits the installation on the device.

If you choose **No**, the client installs on a temporary overlay that clears when the device restarts. In this scenario,

the Endpoint Protection client doesn't fully install until another installation commits changes to the device. This configuration is the default.

Suppress any required computer restarts after the Endpoint Protection client is installed

Choose **Yes** to suppress a computer restart after the Endpoint Protection client installs.

> **IMPORTANT**
> If the Endpoint Protection client requires a computer restart and this setting is **No**, then the computer restarts regardless of any configured maintenance windows.

Allowed period of time users can postpone a required restart to complete the Endpoint Protection installation (hours)

If a restart is necessary after the Endpoint Protection client installs, this setting specifies the number of hours that users can postpone the required restart. This setting requires that the setting for **Suppress any required computer restarts after the Endpoint Protection client is installed** is **No**.

Disable alternate sources (such as Microsoft Windows Update, Microsoft Windows Server Update Services, or UNC shares) for the initial definition update on client computers

Choose **Yes** if you want Configuration Manager to install only the initial definition update on client computers. This setting can be helpful to avoid unnecessary network connections, and reduce network bandwidth, during the initial installation of the definition update.

Enrollment

Polling interval for mobile device legacy clients

Select **Set Interval** to specify the length of time, in minutes or hours, that legacy mobile devices poll for policy. These devices include platforms such as Windows CE, Mac OS X, and Unix or Linux.

Polling interval for modern devices (minutes)

Enter the number of minutes that modern devices poll for policy. This setting is for Windows 10 devices that are managed through on-premises mobile device management.

Allow users to enroll mobile devices and Mac computers

To enable user-based enrollment of legacy devices, set this option to **Yes**, and then configure the following setting:

- **Enrollment profile**: Select **Set Profile** to create or select an enrollment profile. For more information, see Configure client settings for enrollment.

Allow users to enroll modern devices

To enable user-based enrollment of modern devices, set this option to **Yes**, and then configure the following setting:

- **Modern device enrollment profile**: Select **Set Profile** to create or select an enrollment profile. For more information, see Create an enrollment profile that allows users to enroll modern devices.

Hardware inventory

Enable hardware inventory on clients

By default, this setting is **Yes**. For more information, see Introduction to hardware inventory.

Hardware inventory schedule

Select **Schedule** to adjust the frequency that clients run the hardware inventory cycle. By default, this cycle occurs every seven days.

Maximum random delay (minutes)

Specify the maximum number of minutes for the Configuration Manager client to randomize the hardware inventory cycle from the defined schedule. This randomization across all clients helps load-balance inventory processing on the site server. You can specify any value between 0 and 480 minutes. By default, this value is set to 240 minutes (4 hours).

Maximum custom MIF file size (KB)

Specify the maximum size, in kilobytes (KB), allowed for each custom Management Information Format (MIF) file that the client collects during a hardware inventory cycle. The Configuration Manager hardware inventory agent doesn't process any custom MIF files that exceed this size. You can specify a size of 1 KB to 5,120 KB. By default, this value is set to 250 KB. This setting doesn't affect the size of the regular hardware inventory data file.

> **NOTE**
> This setting is available only in the default client settings.

Hardware inventory classes

Select **Set Classes** to extend the hardware information that you collect from clients without manually editing the sms_def.mof file. For more information, see How to configure hardware inventory.

Collect MIF files

Use this setting to specify whether to collect MIF files from Configuration Manager clients during hardware inventory.

For a MIF file to be collected by hardware inventory, it must be in the correct location on the client computer. By default, the files are located in the following paths:

- **IDMIF files** should be in the Windows\System32\CCM\Inventory\Idmif folder.
- **NOIDMIF files** should be in the Windows\System32\CCM\Inventory\Noidmif folder.

> **NOTE**
> This setting is available only in the default client settings.

Metered internet connections

Manage how Windows 8 and later computers use metered internet connections to communicate with Configuration Manager. Internet providers sometimes charge by the amount of data that you send and receive when you are on a metered internet connection.

> **NOTE**
> The configured client setting isn't applied in the following scenarios:
>
> - If the computer is on a roaming data connection, the Configuration Manager client doesn't perform any tasks that require data to be transferred to Configuration Manager sites.
> - If the Windows network connection properties are configured as non-metered, the Configuration Manager client behaves as if the connection is non-metered, and so transfers data to the site.

Client communication on metered internet connections

Choose one of the following options for this setting:

- **Allow**: All client communications are allowed over the metered internet connection, unless the client device

is using a roaming data connection.

- **Limit**: Only the following client communications are allowed over the metered internet connection:
  - Client policy retrieval
  - Client state messages to send to the site
  - Software installation requests from Software Center
  - Required deployments (when the installation deadline is reached)

  > **IMPORTANT**
  > The client always permits software installations from Software Center, regardless of the metered internet connection settings.

  If the client reaches the data transfer limit for the metered internet connection, the client no longer tries to communicate with Configuration Manager sites.

- **Block**: The Configuration Manager client doesn't try to communicate with Configuration Manager sites when it's on a metered internet connection. This option is the default.

Power management

Allow power management of devices

Set this option to **Yes** to enable power management on clients. For more information, see Introduction to power management.

Allow users to exclude their device from power management

Choose **Yes** to let users of Software Center exclude their computer from any configured power management settings.

Allow network wake-up

Added in 1810. When set to **Enable**, configures the power settings on the network adapter to allow the network adapter to wake up the device. When set to **Disable**, the power settings on the network adapter are configured not to allow the network adapter to wake up the device.

Enable wake-up proxy

Specify **Yes** to supplement the site's Wake On LAN setting, when it's configured for unicast packets.

For more information about wake-up proxy, see Plan how to wake up clients.

> **WARNING**
> Don't enable wake-up proxy in a production network without first understanding how it works and evaluating it in a test environment.

Then, configure the following additional settings as needed:

- **Wake-up proxy port number (UDP)**: The port number that clients use to send wake-up packets to sleeping computers. Keep the default port 25536, or change the number to a value of your choice.
- **Wake On LAN port number (UDP)**: Keep the default value of 9, unless you've changed the Wake On LAN (UDP) port number on the **Ports** tab of the site **Properties**.

> **IMPORTANT**
> This number must match the number in the site **Properties**. If you change this number in one place, it isn't automatically updated in the other place.

- **Windows Defender Firewall exception for wake-up proxy**: The Configuration Manager client automatically configures the wake-up proxy port number on devices that run Windows Defender Firewall. Select **Configure** to specify the desired firewall profiles.

  If clients run a different firewall, manually configure it to allow the **Wake-up proxy port number (UDP)**.

- **IPv6 prefixes if required for DirectAccess or other intervening network devices. Use a comma to specify multiple entries**: Enter the necessary IPv6 prefixes for wake-up proxy to function on your network.

Remote tools

Enable Remote Control on clients, and Firewall exception profiles

Select **Configure** to enable the Configuration Manager remote control feature. Optionally, configure firewall settings to allow remote control to work on client computers.

Remote control is disabled by default.

> **IMPORTANT**
> If you don't configure firewall settings, remote control might not work correctly.

Users can change policy or notification settings in Software Center

Choose whether users can change remote control options from within Software Center.

Allow Remote Control of an unattended computer

Choose whether an admin can use remote control to access a client computer that is logged off or locked. Only a logged-on and unlocked computer can be remotely controlled when this setting is disabled.

Prompt user for Remote Control permission

Choose whether the client computer shows a message asking for the user's permission before allowing a remote control session.

Prompt user for permission to transfer content from shared clipboard

Before transferring content from the shared clipboard in a remote control session, allow your users the opportunity to accept or deny file transfers. Users only need to grant permission once per session. The viewer can't give themselves permission to transfer the file.

Grant Remote Control permission to local Administrators group

Choose whether local admins on the server that initiates the remote control connection can establish remote control sessions to client computers.

Access level allowed

Specify the level of remote control access to allow. Choose from the following settings:

- **No Access**
- **View Only**
- **Full Control**

Permitted viewers of Remote Control and Remote Assistance

Select **Set Viewers** to specify the names of the Windows users who can establish remote control sessions to client computers.

Show session notification icon on taskbar

Configure this setting to **Yes** to show an icon on the client's Windows taskbar to indicate an active remote control session.

Show session connection bar

Set this option to **Yes** to show a high-visibility session connection bar on clients, to indicate an active remote control session.

Play a sound on client

Set this option to use sound to indicate when a remote control session is active on a client computer. Select one of the following options:

- **No sound**
- **Beginning and send of session** (default)
- **Repeatedly during session**

Manage unsolicited Remote Assistance settings

Configure this setting to **Yes** to let Configuration Manager manage unsolicited Remote Assistance sessions.

In an unsolicited Remote Assistance session, the user at the client computer didn't request assistance to initiate the session.

Manage solicited Remote Assistance settings

Set this option to **Yes** to let Configuration Manager manage solicited Remote Assistance sessions.

In a solicited Remote Assistance session, the user at the client computer sent a request to the admin for remote assistance.

Level of access for Remote Assistance

Choose the level of access to assign to Remote Assistance sessions that are initiated in the Configuration Manager console. Select one of the following options:

- **None** (default)
- **Remote Viewing**
- **Full Control**

> **NOTE**
> The user at the client computer must always grant permission for a Remote Assistance session to occur.

Manage Remote Desktop settings

Set this option to **Yes** to let Configuration Manager manage Remote Desktop sessions for computers.

Allow permitted viewers to connect by using Remote Desktop connection

Set this option to **Yes** to add users specified in the permitted viewer list to the Remote Desktop local user group on clients.

Require network level authentication on computers that run Windows Vista operating system and later versions

Set this option to **Yes** to use network-level authentication (NLA) to establish Remote Desktop connections to client computers. NLA initially requires fewer remote computer resources, because it finishes user authentication before it establishes a Remote Desktop connection. Using NLA is a more secure configuration. NLA helps protect the

computer from malicious users or software, and it reduces the risk from denial-of-service attacks.

Software Center

Select these new settings to specify company information

Set this option to **Yes**, and then specify the following settings to brand Software Center for your organization:

- **Company name**: Enter the organization name that users see in Software Center.
- **Color scheme for Software Center**: Click **Select Color** to define the primary color used by Software Center.
- **Select a logo for Software Center**: Click **Browse** to select an image to appear in Software Center. The logo must be a JPEG, PNG, or BMP of 400 x 100 pixels, with a maximum size of 750 KB. The logo file name shouldn't contain spaces.

Hide unapproved applications in Software Center

When you enable this option, user-available applications that require approval are hidden in Software Center.

Hide installed applications in Software Center

When you enable this option, applications that are already installed no longer show in the Applications tab. This option is set as the default when you install or upgrade to Configuration Manager 1802. Installed applications are still available for review under the installation status tab.

Hide Application Catalog link in Software Center

Starting in Configuration Manager version 1806, you can specify the visibility of the application catalog web site link in Software Center. When this option is set, users won't see the application catalog web site link in the Installation status node of Software Center.

Software Center tab visibility

Starting in version 1906

Choose which tabs should be visible in Software Center. Use the **Add** button to move a tab to **Visible tabs**. Use the **Remove** button to move it to the **Hidden tabs** list. Order the tabs using the **Move Up** or **Move Down** buttons.

Available tabs:

- **Applications**
- **Updates**
- **Operating Systems**
- **Installation Status**
- **Device Compliance**
- **Options**
- Add up to 5 custom tabs by clicking the **Add tab** button.
    - Specify the **Tab name** and **Content URL** for your custom tab.
    - Click **Delete Tab** to remove a custom tab.

> **IMPORTANT**
>
> - Some website features may not work when using it as a custom tab in Software Center. Make sure to test the results before deploying this to clients.
> - Specify only trusted or intranet website addresses when you add a custom tab.

Version 1902 and earlier

Configure the additional settings in this group to **Yes** to make the following tabs visible in Software Center:

- **Applications**
- **Updates**
- **Operating Systems**
- **Installation Status**
- **Device Compliance**
- **Options**
- **Specify a custom tab for Software Center** (starting in version 1806)
  - **Tab name**
  - **Content URL**

> **IMPORTANT**
>
> Some website features may not work when using it as a custom tab in Software Center. Make sure to test the results before deploying this to clients.
>
> Specify only trusted or intranet website addresses when you add a custom tab.

For example, if your organization doesn't use compliance policies, and you want to hide the Device Compliance tab in Software Center, set **Enable Device Compliance tab** to **No**.

Configure default views in Software Center

(Introduced in version 1902)

- Configure the **Default application filter** as either **All** or only **Required** applications.
  - Software Center always uses your default setting. Users can change this filter, but Software Center doesn't persist their preference.
- Set the **Default application view** as either **Tile view** or **List view**.
  - If a user changes this configuration, Software Center persists the user's preference in the future.

Software deployment

Schedule re-evaluation for deployments

Configure a schedule for when Configuration Manager reevaluates the requirement rules for all deployments. The default value is every seven days.

> **IMPORTANT**
> This setting is more invasive to the local client than it is to the network or site server. A more aggressive reevaluation schedule negatively affects the performance of your network and client computers. Microsoft doesn't recommend setting a lower value than the default. If you change this value, closely monitor performance.

Initiate this action from a client as follows: in the **Configuration Manager** control panel, from the **Actions** tab, select **Application Deployment Evaluation Cycle**.

Software inventory

Enable software inventory on clients

This option is set to **Yes** by default. For more information, see Introduction to software inventory.

Schedule software inventory and file collection

Select **Schedule** to adjust the frequency that clients run the software inventory and file collection cycles. By default, this cycle occurs every seven days.

Inventory reporting detail

Specify one of the following levels of file information to inventory:

- **File only**
- **Product only**
- **Full details** (default)

Inventory these file types

If you want to specify the types of file to inventory, select **Set Types**, and then configure the following options:

> **NOTE**
> If multiple custom client settings are applied to a computer, the inventory that each setting returns is merged.

- Select **New** to add a new file type to inventory. Then specify the following information in the **Inventoried File Properties** dialog box:
  - **Name**: Provide a name for the file that you want to inventory. Use an asterisk (`*`) wildcard to represent any string of text, and a question mark (`?`) to represent any single character. For example, if you want to inventory all files with the extension .doc, specify the file name `*.doc`.
  - **Location**: Select **Set** to open the **Path Properties** dialog box. Configure software inventory to search all client hard disks for the specified file, search a specified path (for example, `C:\Folder`), or search for a specified variable (for example, `%windir%`). You can also search all subfolders under the specified path.
  - **Exclude encrypted and compressed files**: When you choose this option, any compressed or encrypted files aren't inventoried.
  - **Exclude files in the Windows folder**: When you choose this option, any files in the Windows folder and its subfolders aren't inventoried.

  Select **OK** to close the **Inventoried File Properties** dialog box. Add all the files that you want to inventory, and then select **OK** to close the **Configure Client Setting** dialog box.

Collect files

If you want to collect files from client computers, select **Set Files**, and then configure the following settings:

> **NOTE**
> If multiple custom client settings are applied to a computer, the inventory that each setting returns is merged.

- In the **Configure Client Setting** dialog box, select **New** to add a file to be collected.
- In the **Collected File Properties** dialog box, provide the following information:
  - **Name**: Provide a name for the file that you want to collect. Use an asterisk (`*`) wildcard to represent any string of text, and a question mark (`?`) to represent any single character.
  - **Location**: Select **Set** to open the **Path Properties** dialog box. Configure software inventory to search all client hard disks for the file that you want to collect, search a specified path (for example, `C:\Folder`), or search for a specified variable (for example, `%windir%`). You can also search all subfolders under the specified path.
  - **Exclude encrypted and compressed files**: When you choose this option, any compressed or encrypted files aren't collected.
  - **Stop file collection when the total size of the files exceeds (KB)**: Specify the file size, in kilobytes (KB), after which the client stops collecting the specified files.

> **NOTE**
> The site server collects the five most recently changed versions of collected files, and stores them in the `<ConfigMgr installation directory>\Inboxes\Sinv.box\Filecol` directory. If a file hasn't changed since the last software inventory cycle, the file isn't collected again.
>
> Software inventory doesn't collect files larger than 20 MB.
>
> The value **Maximum size for all collected files (KB)** in the **Configure Client Setting** dialog box shows the maximum size for all collected files. When this size is reached, file collection stops. Any files already collected are retained and sent to the site server.

> **IMPORTANT**
> If you configure software inventory to collect many large files, this configuration might negatively affect the performance of your network and site server.

For information about how to view collected files, see How to use Resource Explorer to view software inventory.

Select **OK** to close the **Collected File Properties** dialog box. Add all the files that you want to collect, and then select **OK** to close the **Configure Client Setting** dialog box.

Set Names

The software inventory agent retrieves manufacturer and product names from file header information. These names aren't always standardized in the file header information. When you view software inventory in Resource Explorer, different versions of the same manufacturer or product name can appear. To standardize these display names, select **Set Names**, and then configure the following settings:

- **Name type**: Software inventory collects information about both manufacturers and products. Choose whether you want to configure display names for a **Manufacturer** or a **Product**.

- **Display name**: Specify the display name that you want to use in place of the names in the **Inventoried names** list. To specify a new display name, select **New**.
- **Inventoried names**: To add an inventoried name, select **New**. This name is replaced in software inventory by the name chosen in the **Display name** list. You can add multiple names to replace.

Software Metering

Enable software metering on clients

This setting is set to **Yes** by default. For more information, see Software metering.

Schedule data collection

Select **Schedule** to adjust the frequency that clients run the software metering cycle. By default, this cycle occurs every seven days.

Software updates

Enable software updates on clients

Use this setting to enable software updates on Configuration Manager clients. When you disable this setting, Configuration Manager removes existing deployment policies from clients. When you re-enable this setting, the client downloads the current deployment policy.

> **IMPORTANT**
> When you disable this setting, compliance policies that rely on software updates will no longer function.

Software update scan schedule

Select **Schedule** to specify how often the client initiates a compliance assessment scan. This scan determines the state for software updates on the client (for example, required or installed). For more information about compliance assessment, see Software updates compliance assessment.

By default, this scan uses a simple schedule to initiate every seven days. You can create a custom schedule. You can specify an exact start day and time, use Universal Coordinated Time (UTC) or the local time, and configure the recurring interval for a specific day of the week.

> **NOTE**
> If you specify an interval of less than one day, Configuration Manager automatically defaults to one day.

> **WARNING**
> The actual start time on client computers is the start time plus a random amount of time, up to two hours. This randomization prevents client computers from initiating the scan and simultaneously connecting to the active software update point.

Schedule deployment re-evaluation

Select **Schedule** to configure how often the software updates client agent reevaluates software updates for installation status on Configuration Manager client computers. When previously installed software updates are no longer found on clients but are still required, the client reinstalls the software updates.

Adjust this schedule based on company policy for software update compliance, and whether users can uninstall software updates. Every deployment re-evaluation cycle results in network and client computer processor activity.

By default, this setting uses a simple schedule to initiate the deployment re-evaluation scan every seven days.

> **NOTE**
> If you specify an interval of less than one day, Configuration Manager automatically defaults to one day.

When any software update deployment deadline is reached, install all other software update deployments with deadline coming within a specified period of time

Set this option to **Yes** to install all software updates from required deployments with deadlines occurring within a specified period of time. When a required software update deployment reaches a deadline, the client initiates installation for the software updates in the deployment. This setting determines whether to install software updates from other required deployments that have a deadline within the specified time.

Use this setting to expedite installation for required software updates. This setting also has the potential to increase client security, decrease notifications to the user, and decrease client restarts. By default, this setting is set to **No**.

Period of time for which all pending deployments with deadline in this time will also be installed

Use this setting to specify the period of time for the previous setting. You can enter a value from 1 to 23 hours, and from 1 to 365 days. By default, this setting is configured for seven days.

Allow clients to download delta content when available

(Introduced in version 1902)

Set this option to **Yes** to allow clients to use delta content files. This setting allows the Windows Update Agent on the device to determine what content is needed and selectively download it.

> **NOTE**
> This client setting replaces **Enable installation of Express installation files on clients**. Set this option to **Yes** to allow clients to use express installation files. For more information, see Manage Express installation files for Windows 10 updates.

Port that clients use to receive requests for delta content

(Introduced in version 1902)

This setting configures the local port for the HTTP listener to download delta content. It's set to 8005 by default. You don't need to open this port in the client firewall.

> **NOTE**
> This client setting replaces **Port used to download content for Express installation files**.

Enable management of the Office 365 Client Agent

When you set this option to **Yes**, it enables the configuration of Office 365 installation settings. It also enables downloading files from Office Content Delivery Networks (CDNs), and deploying the files as an application in Configuration Manager. For more information, see Manage Office 365 ProPlus.

Enable installation of software updates in "All deployments" maintenance window when "Software Update" maintenance window is available

When you set this option to **Yes** and the client has at least one "Software Update" maintenance window defined, software updates will install during an "All deployments" maintenance window. By default, this setting is set to **No**. This client setting was added in Configuration Manager version 1810.

Specify thread priority for feature updates

Starting in Configuration Manager version 1902, you can adjust the priority with which Windows 10 version 1709 or later clients install a feature update through Windows 10 servicing. This setting has no impact on Windows 10 in-place upgrade task sequences.

This client setting provides the following options:

- **Not Configured**: Configuration Manager doesn't change the setting. Admins can pre-stage their own setupconfig.ini file. This value is the default.
- **Normal**: Windows Setup uses more system resources and updates faster. It uses more processor time, so the total installation time is shorter, but the user's outage is longer.
  - Configures the setupconfig.ini file on the device with the `/Priority Normal` Windows setup command-line option.
- **Low**: You can continue to work on the device while it downloads and updates in the background. The total installation time is longer, but the user's outage is shorter. You may need to increase the update max run time to avoid a time out when using this option.
  - Removes the `/Priority` Windows setup command-line option from the setupconfig.ini file.

Enable third party software updates

When you set this option to **Yes**, it sets the policy for **Allow signed updates for an intranet Microsoft update service location** and installs the signing certificate to the Trusted Publisher store on the client.

Enable Dynamic Update for feature updates

Starting in Configuration Manager version 1906, you can configure Dynamic Update for Windows 10. Dynamic Update installs language packs, features on demand, drivers, and cumulative updates during Windows setup by directing the client to download these updates from the internet. When this setting is set to either **Yes** or **No**, Configuration Manager modifies the setupconfig file that is used during feature update installation.

- **Not Configured** - The default value. No changes are made to the setupconfig file.
  - Dynamic Update is enabled by default on all supported versions of Windows 10.
    - For Windows 10 versions 1803 and prior, Dynamic Update checks the device's WSUS server for approved dynamic updates. In Configuration Manager environments, dynamic updates are never directly approved in the WSUS server so these devices don't install them.
    - Starting with Windows 10 version 1809, Dynamic Update uses the device's internet connection to get dynamic updates from Microsoft Update. These dynamic updates aren't published for WSUS use.
- **Yes** - Enables Dynamic Update.
- **No** - Disables Dynamic Update.

State Messaging

State message reporting cycle (minutes)

Specifies how often clients report state messages. This setting is 15 minutes by default.

User and device affinity

User device affinity usage threshold (minutes)

Specify the number of minutes before Configuration Manager creates a user device affinity mapping. By default, this value is 2880 minutes (two days).

User device affinity usage threshold (days)

Specify the number of days over which the client measures the threshold for usage-based device affinity. By

default, this value is 30 days.

> **NOTE**
>
> For example, you specify **User device affinity usage threshold (minutes)** as **60** minutes, and **User device affinity usage threshold (days)** as **5** days. Then the user must use the device for 60 minutes over a period of 5 days to create automatic affinity with the device.

Automatically configure user device affinity from usage data

Choose **Yes** to create automatic user device affinity based on the usage information that Configuration Manager collects.

Allow user to define their primary devices

When this setting is **Yes**, users can identify their own primary devices in Software Center. For more information, see the Software Center user guide.

Windows Analytics

For more information on these settings, see Configure Clients to report data to Windows Analytics.

Device restart notifications in Configuration Manager

8/23/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (current branch)

The notifications a user receives for a pending device restart can vary depending on Computer restart client settings and which version of Configuration Manager is being used. This article helps admins determine what the user experience is for pending device restart notifications.

NOTE

- This article focuses on client settings found in Configuration Manager version 1902 and version 1906.

Deployment types for restart notifications

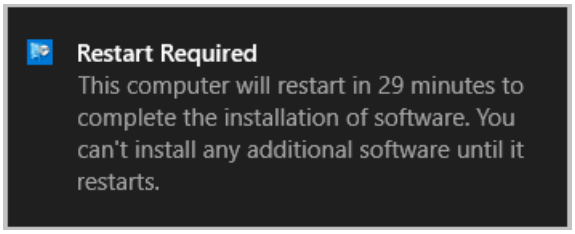
The Computer restart client settings change the user experience for all required deployments that require a restart of the following types:

- Application
- Task sequence
- Software update

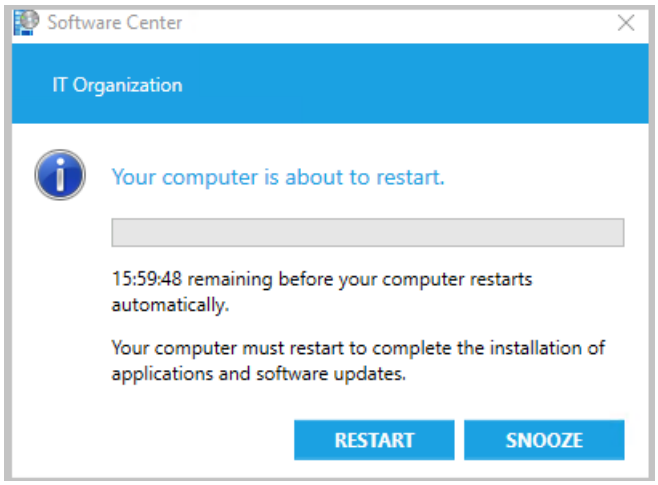
Restart notification types

When a restart is required, the end user is given notification of the upcoming restart. There are four general notifications users can receive:

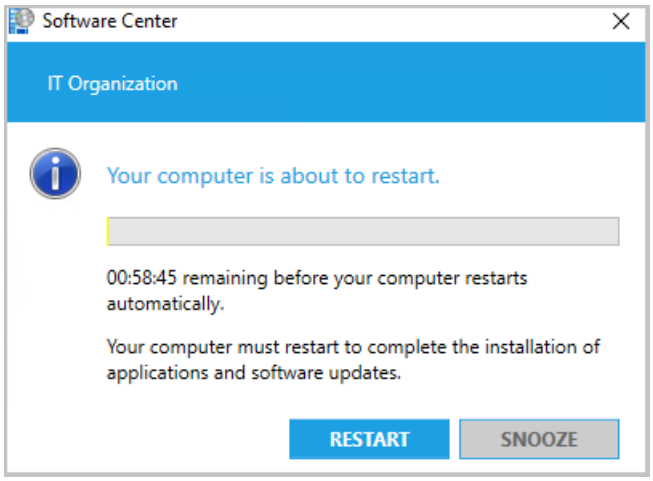
Toast notification informing you a restart is needed. The information in the toast notification can be different depending on which version of Configuration Manager you're running. This type of notification is native to the Windows OS and you may also see third-party software using this type of notification.



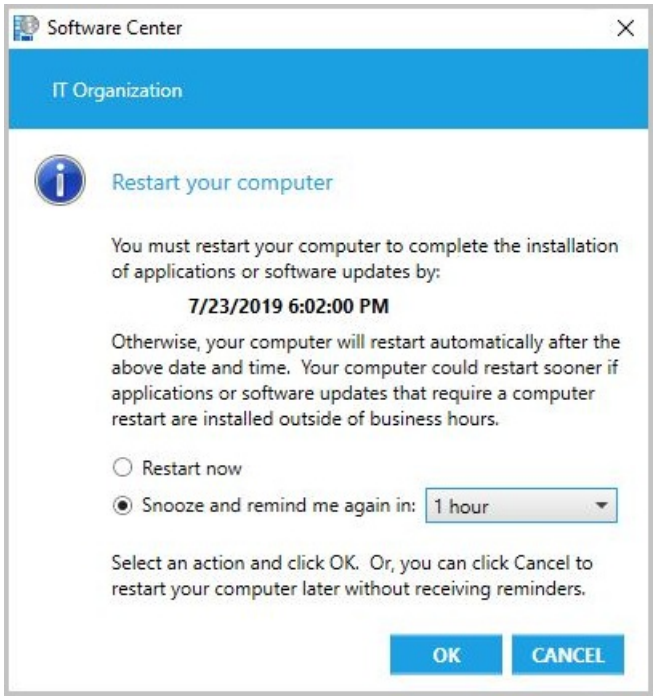
Software Center notification with a snooze option showing time remaining before a restart is enforced. The message may be different depending on your version of Configuration Manager.



Software Center final countdown notification that can't be closed by the user. The snooze button is grayed out.

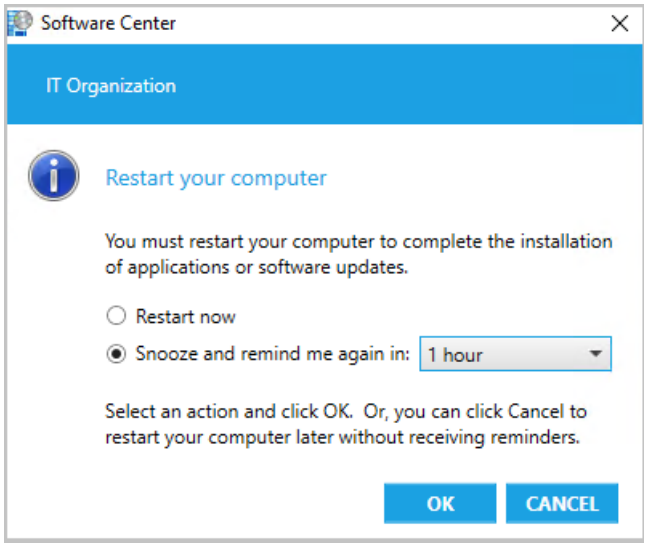


If the user proactively installs required software that needs restart before the deadline occurs, they'll see a different notification. The following notification occurs when both the user experience setting allows notifications and you don't use toast notifications for the deployment. For more information about configuring these settings, see Deployment **User Experience** settings and User notifications for required deployments.



- When you don't use toast notifications, the dialog for software marked as **Available** is similar to proactively installed software.

- For **Available** software, the notification doesn't have a deadline for the restart and the user can choose their own snooze interval. For more information, see Approval settings.



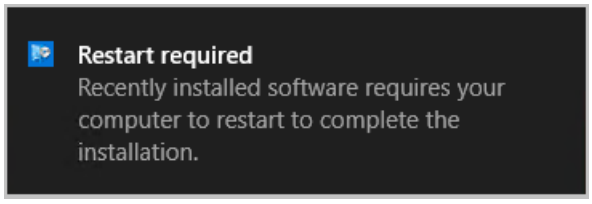
Device restart notifications in version 1902

Sometimes users don't see the Windows toast notification about a restart or required deployment. Then they don't see the experience to snooze the reminder. This behavior can lead to a poor user experience when the client reaches a deadline.

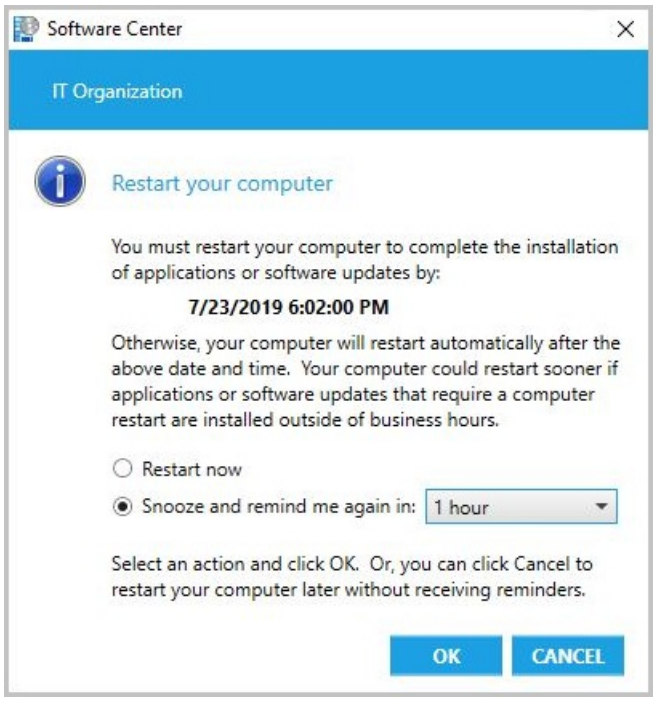
Starting in version 1902, when software changes are required or deployments need a restart, you have the option of using a more intrusive dialog window.

In the Computer Restart group of client settings, enable the following option: **When a deployment requires a restart, show a dialog window to the user instead of a toast notification**.

Configuring this client setting changes the user experience for all required deployments that require a restart from toast notifications:

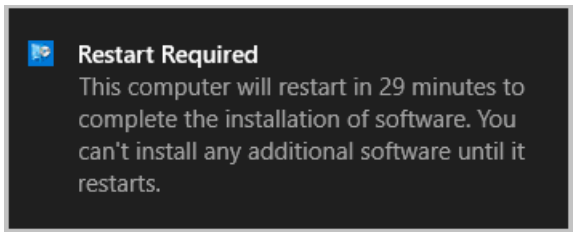


To the more intrusive Software Center dialog window:

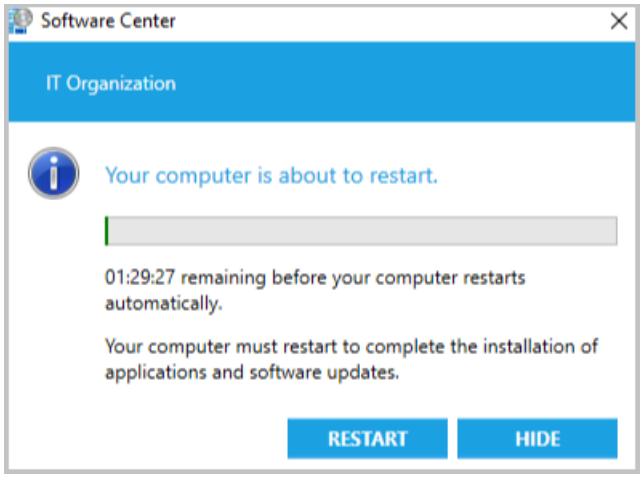


If the user didn't restart their device after the installation, then they'll get a notification as a reminder. This temporary reminder will appear to the user based on the client setting: **Display a temporary notification to the user that indicates the interval before the user is logged off or the computer restarts (minutes)**. This setting is the overall time the user has to restart the machine before a restart is forced.

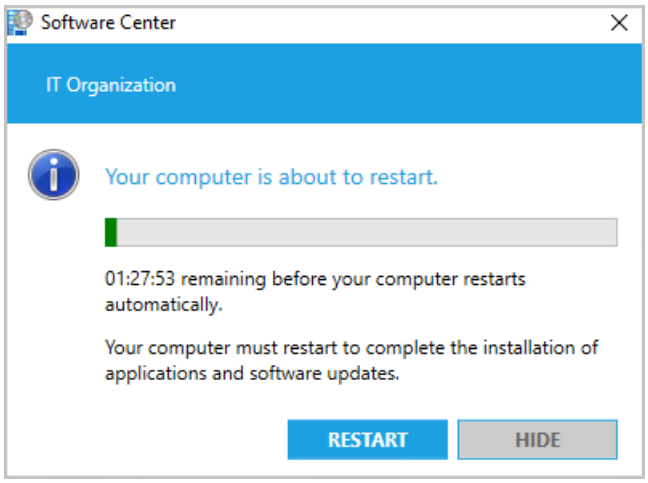
- Temporary notification when you use toast notifications:



- Temporary notification when you use Software Center dialog window, not toast:



If the user doesn't restart after the temporary notification, they'll be given the final countdown notification that they can't close. The timing of when the final notification appears is based on the client setting: **Display a dialog box that the user cannot close, which displays the countdown interval before the user is logged off or the computer restarts (minutes)**. For instance, if the setting is 60, then an hour before a reboot is forced, the final notification appears to the user:



The following settings must be shorter in duration than the shortest maintenance window applied to the computer:

- **Display a temporary notification to the user that indicates the interval before the user is logged off or the computer restarts (minutes)**
- **Display a dialog box that the user cannot close, which displays the countdown interval before the user is logged off or the computer restarts (minutes)**

> **IMPORTANT**
> In Configuration Manager 1902, under certain circumstances, the dialog box won't replace toast notifications. To resolve this issue, install the update rollup for Configuration Manager version 1902.

Device restart notifications starting in version 1906

Some admins prefer frequent restart notifications and a short time frame for allowing restarts to be postponed. Other admins allow users to postpone a restart for longer periods of time and want users to be notified of the pending restart infrequently. Configuration Manager version 1906 gives an admin additional control over the timing and frequency of restart notifications. The following items were introduced in 1906 to give the admin greater control:

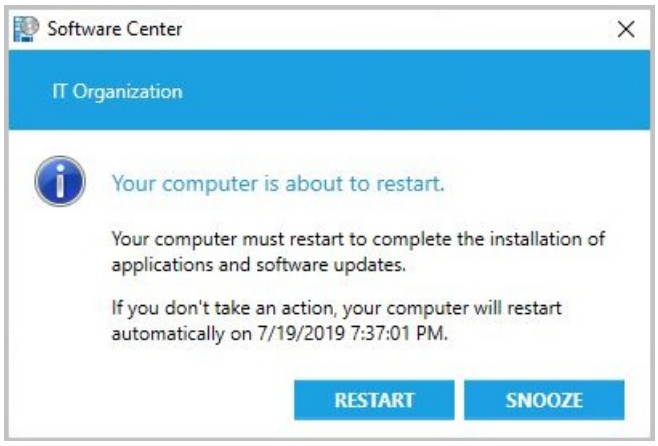
- **Specify the snooze duration for computer restart countdown notifications (minutes)** was added to Computer restart client settings.
- The maximum value for **Display a temporary notification to the user that indicates the interval before the user is logged off or the computer restarts (minutes)** increased from 1440 minutes (24 hours) to 20160 minutes (two weeks).
- The user won't see a progress bar in the restart notification until the pending restart is less than 24 hours away.

Notifications when required software is installed at or after the deadline

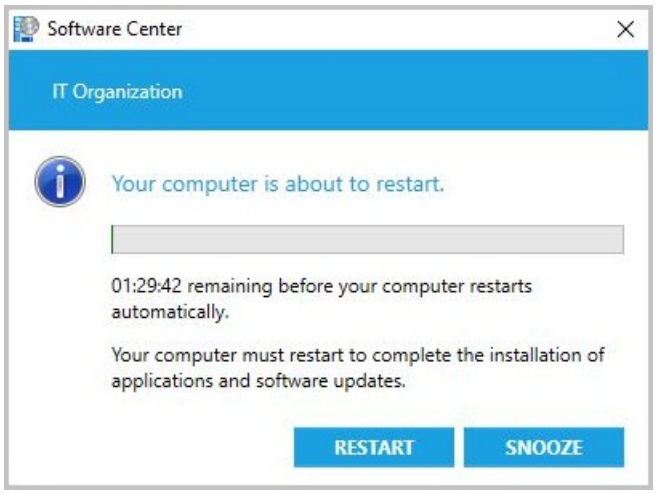
When required software is installed at or after the deadline, your users will see notifications depending on what client settings you selected.

If the setting **When a deployment requires a restart, show a dialog window to the user instead of a toast notification** is set to:

- **No** - Toast notifications are used until the final countdown notification is reached.
- **Yes** - A Software Center notification is seen.
  - If the restart is greater than 24 hours away, an estimated restart time is seen. The timing of this notification is based on the setting: **Display a temporary notification to the user that indicates the interval before the user is logged off or the computer restarts (minutes)**.

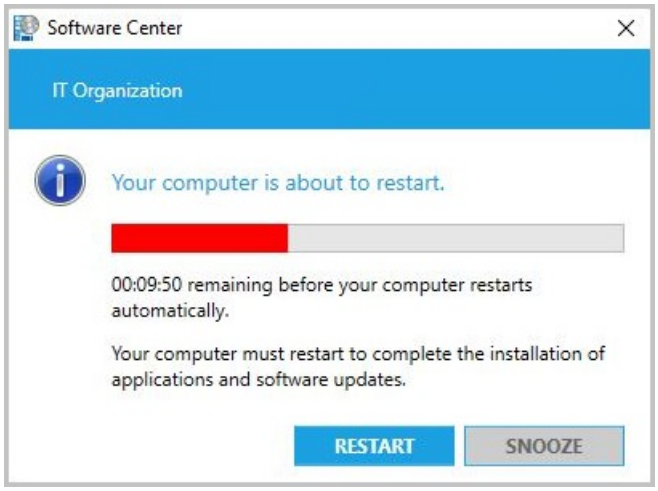


- If the restart is less than 24 hours away, a progress bar is seen. The timing of this notification is based on the setting: **Display a temporary notification to the user that indicates the interval before the user is logged off or the computer restarts (minutes)**



If the user selects the **Snooze** button, another temporary notification will occur after the snooze period elapses, assuming they haven't yet reached the final countdown. The timing of the next notification is based on the setting: **Specify the snooze duration for computer restart countdown notifications (hours)**. If the user selects **Snooze** and your snooze interval is one hour, then the user will be notified again in 60 minutes assuming they haven't yet reached the final countdown.

When the final countdown is reached, the user is given a notification they can't close. The progress bar is in red and the user can't hit **Snooze**.

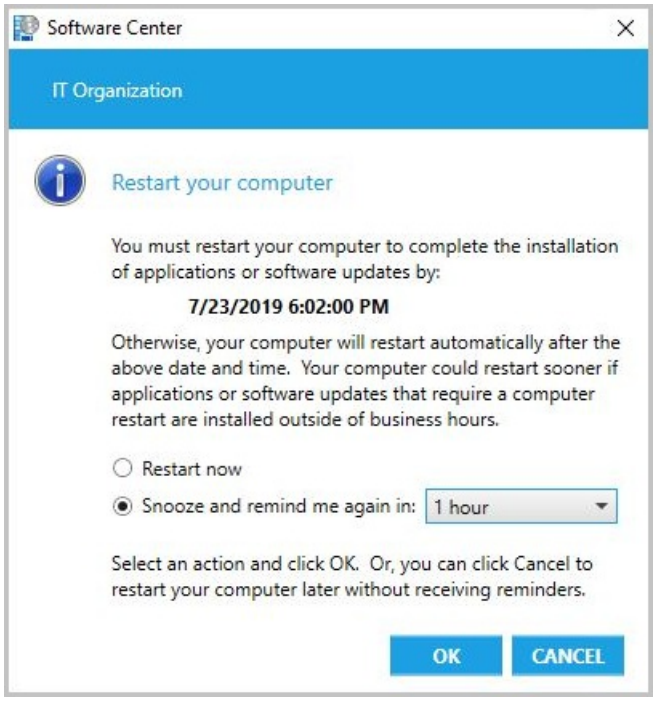


The user proactively installs before the deadline

If the user proactively installs required software that needs restart before the deadline occurs, they'll see a different notification. For more information about configuring these settings, see Deployment **User Experience** settings

and User notifications for required deployments.

The following notification occurs when both the user experience setting allows notifications and you don't use toast notifications for the deployment:



Once the deadline for the software is reached, the Notifications when required software is installed at or after the deadline behavior is followed.

Log files

Use the **RebootCoordinator.log** and **SCNotify.log** for troubleshooting device restarts. You may also have to use additional client log files based on the type of deployment used.

Next steps

- Introduction application management
- Introduction to operating system deployment
- Introduction to software updates management

How to configure Wake on LAN in System Center Configuration Manager

8/8/2019 • 7 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Specify Wake on LAN settings for System Center Configuration Manager when you want to bring computers out of a sleep state.

Wake on LAN starting in version 1810

Starting in Configuration Manager 1810, there's a new way to wake up sleeping machines. You can wake up clients from the Configuration Manager console, even if the client isn't on the same subnet as the site server. If you need to do maintenance or query devices, you're not limited by remote clients that are asleep. The site server uses the client notification channel to identify other clients that are awake on the same remote subnet, then uses those clients to send a wake on LAN request (magic packet). Using the client notification channel helps avoid MAC flaps, which could cause the port to be shut down by the router. The new version of Wake on LAN can be enabled at the same time as the older version.

Limitations

- At least one client in the target subnet must be awake.
- This feature doesn't support the following network technologies:
  - IPv6
  - 802.1x network authentication

    > **NOTE**
    > 802.1x network authentication may work with additional configuration depending on the hardware and its configuration.

- Machines only wake when you notify them through the **Wake Up** client notification.
  - For wake-up when a deadline occurs, the older version of Wake on LAN is used.
  - If the older version isn't enabled, client wake up won't occur for deployments created with the settings **Use Wake-on-LAN to wake up clients for required deployments** or **Send wake-up packets**.

Security role permissions

- **Notify resource** under the Collection category

Configure the clients to use Wake on LAN starting in version 1810

Previously you had to manually enable the client for wake on LAN in the properties of the network adapter. Configuration Manager 1810 includes a new client setting called **Allow network wake-up**. Configure and deploy this setting instead of modifying the properties of the network adapter.

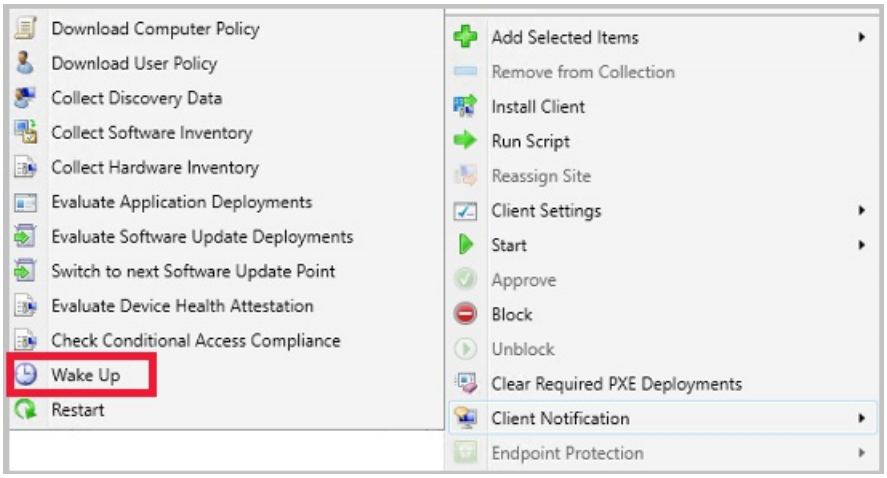
1. Under **Administration**, go to **Client Settings**.
2. Select the client settings you want to edit, or create new custom client settings to deploy. For more information, see How to configure client settings.
3. Under the **Power Management** client settings, select **Enable** for the **Allow network wake-up** setting. For more information about this setting, see About client settings.

4. Starting in Configuration Manager 1902, the new version of Wake on LAN honors the custom UDP port you specify for the **Wake On LAN port number (UDP)** client setting. This setting is shared by both the new and older version of Wake on LAN.

Wake up a client using client notification starting in 1810

You can wake up a single client or any sleeping clients in a collection. For devices that are already awake in the collection, no action is taken for them. Only clients that are asleep will be sent a Wake on LAN request. For more information on how to notify a client to wake, see Client notification.

- **To wake up a single client:** Right-click on the client, go to **Client Notification**, then select **Wake up**.



- **To wake up all sleeping clients in a collection:** Right-click on the device collection, go to **Client Notification**, then select **Wake up**.
  - This action can't be run on built-in collections.
  - When you have a mix of asleep and awake clients in a collection, only the clients that are asleep are sent a Wake on LAN request.
  - This action is only active when the Configuration Manager console is connected to a stand-alone or child primary site. When connected to a Central Administration Site, the action is not available.

What to expect when only the new version of Wake on LAN is enabled

When you have only the new version of Wake on LAN enabled, only the **Wake Up** client notification is enabled. Clients aren't sent a notification when a deadline is received on deployments such as task sequences, software distribution, or software updates installation. Once a sleeping machine is back online, it will be reflected in the console when it checks in with the Management Point.

Starting in Configuration Manager version 1902, you can specify the Wake on LAN port. This setting is shared by both the new and older version of Wake on LAN.

What to expect when both versions of Wake on LAN are enabled

When you have both versions of Wake on LAN enabled, you can use the **Wake Up** client notification and wake up on deadline. The client notification functions a little differently than traditional Wake on LAN. For a brief explanation of how the client notification works, see the Wake on LAN starting in version 1810 section. The new client setting **Allow network wake-up** will change the NIC properties to allow Wake on LAN. You no longer need to manually change it for new machines that are added to your environment. All other functionality of Wake on LAN hasn't been changed.

Starting in version 1902, the **Wake Up** client notification honors your existing **Wake On LAN port number (UDP)** setting.

Wake on LAN for version 1806 and earlier

Specify Wake on LAN settings for System Center Configuration Manager when you want to bring computers out of a sleep state to install required software, such as software updates, applications, task sequences, and programs.

You can supplement Wake on LAN by using the wake-up proxy client settings. However, to use wake-up proxy, you must first enable Wake on LAN for the site and specify **Use wake-up packets only** and the **Unicast** option for the Wake on LAN transmission method. This wake-up solution also supports ad-hoc connections, such as a remote desktop connection.

Use the first procedure to configure a primary site for Wake on LAN. Then, use the second procedure to configure the wake-up proxy client settings. This second procedure configures the default client settings for the wake-up proxy settings to apply to all computers in the hierarchy. If you want these settings to apply to only selected computers, create a custom device setting and assign it to a collection that contains the computers that you want to configure for wake-up proxy. For more information about how to create custom client settings, see How to configure client settings in System Center Configuration Manager.

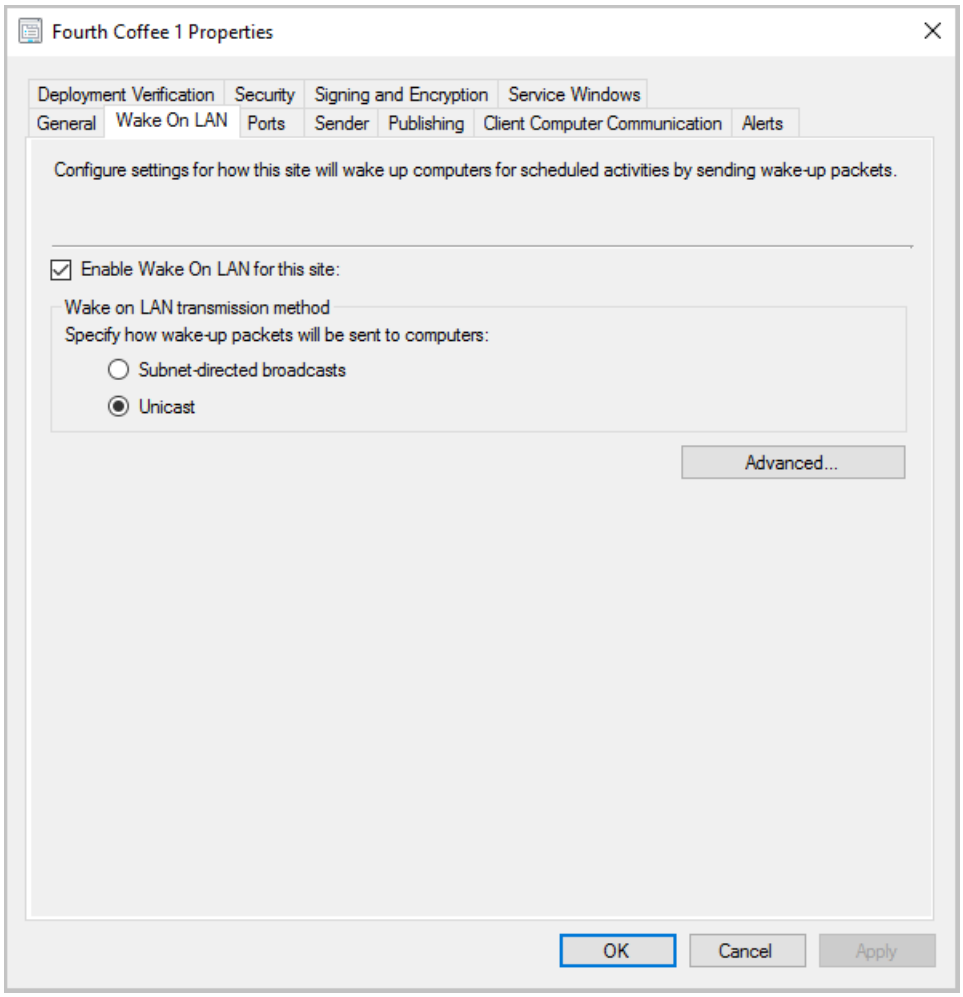
A computer that receives the wake-up proxy client settings will likely pause its network connection for 1-3 seconds. This occurs because the client must reset the network interface card to enable the wake-up proxy driver on it.

> **WARNING**
> To avoid unexpected disruption to your network services, first evaluate wake-up proxy on an isolated and representative network infrastructure. Then use custom client settings to expand your test to a selected group of computers on several subnets. For more information about how wake-up proxy works, see Plan how to wake up clients in System Center Configuration Manager.

To configure Wake on LAN for a site for version 1806 and earlier

To use Wake on LAN, you need to enable it for each site in a hierarchy.

1. In the Configuration Manager console, go to **Administration > Site Configuration > Sites**.
2. Click the primary site to configure, and then click **Properties**.
3. Click the **Wake on LAN** tab, and configure the options that you require for this site. To support wake-up proxy, make sure you select **Use wake-up packets only** and **Unicast**. For more information, see Plan how to wake up clients in System Center Configuration Manager.
4. Click **OK** and repeat the procedure for all primary sites in the hierarchy.



To configure wake-up proxy client settings

1. In the Configuration Manager console, go to **Administration > Client Settings**.
2. Click **Default Client Settings**, and then click **Properties**.
3. Select **Power Management** and then choose **Yes** for **Enable wake-up proxy**.
4. Review and if necessary, configure the other wake-up proxy settings. For more information on these settings, see Power management settings.
5. Click **OK** to close the dialog box, and then click **OK** to close the Default Client Settings dialog box.

You can use the following Wake On LAN reports to monitor the installation and configuration of wake-up proxy:

- Wake-Up Proxy Deployment State Summary
- Wake-Up Proxy Deployment State Details

> **TIP**
>
> To test whether wake-up proxy is working, test a connection to a sleeping computer. For example, connect to a shared folder on that computer, or try connecting to the computer using Remote Desktop. If you use Direct Access, check that the IPv6 prefixes work by trying the same tests for a sleeping computer that is currently on the Internet.

How to deploy clients to Windows computers in Configuration Manager

9/5/2019 • 25 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article provides details on how to deploy the Configuration Manager client to Windows computers. For more information on planning and preparing for client deployment, see these articles:

- Client installation methods
- Prerequisites for deploying clients to Windows computers
- Security and privacy for Configuration Manager clients
- Best practices for client deployment

Client push installation

There are three main ways to use client push:

- When you configure client push installation for a site, client installation automatically runs on computers that the site discovers. This method is scoped to the site's configured boundaries when those boundaries are configured as a boundary group.
- Start client push installation by running the Client Push Installation Wizard for a specific collection or resource within a collection.
- Use the Client Push Installation Wizard to install the Configuration Manager client, which you can use to query the result. The installation will succeed only if one of the items returned by the query is the **ResourceID** attribute of the **System Resource** class.

If the site server can't contact the client computer or start the setup process, it automatically retries the installation every hour. The server continues to retry for up to seven days.

To help track the client installation process, install a fallback status point before you install the clients. When you install a fallback status point, it's automatically assigned to clients when they're installed by the client push installation method. To track client installation progress, view the client deployment and assignment reports.

Client log files provide more detailed information for troubleshooting. The log files don't require a fallback status point. For example, the CCM.log file on the site server records any problems that occur when the site server connects to the computer. The CCMSetup.log file on the client records the installation process.

> **IMPORTANT**
> Client push only succeeds if all prerequisites are met. For more information, see Installation method dependencies.

Configure the site to automatically use client push for discovered computers

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. Select the site for which you want to configure automatic site-wide client push installation.
3. On the **Home** tab of the ribbon, in the **Settings** group, select **Client Installation Settings**, and then select

Client Push Installation.

4. On the **General** tab of the Client Push Installation Properties window, select **Enable automatic site-wide client push installation**.

5. Starting in version 1806, when you update the site, a Kerberos check for client push is enabled. The option to **Allow connection fallback to NTLM** is enabled by default, which is consistent with previous behavior. If the site can't authenticate the client by using Kerberos, it retries the connection by using NTLM. The recommended configuration for improved security is to disable this setting, which requires Kerberos without NTLM fallback.

   > **NOTE**
   >
   > When it uses client push to install the Configuration Manager client, the site server creates a remote connection to the client. Starting in version 1806, the site can require Kerberos mutual authentication by not allowing fallback to NTLM before establishing the connection. This enhancement helps to secure the communication between the server and the client.
   >
   > Depending on your security policies, your environment might already prefer or require Kerberos over the older NTLM authentication. For more information on the security considerations of these authentication protocols, read about the Windows security policy setting to restrict NTLM.
   >
   > To use this feature, clients must be in a trusted Active Directory forest. Kerberos in Windows relies on Active Directory for mutual authentication.

6. Select the system types to which Configuration Manager should push the client software. Select whether you want to install the client on domain controllers.

7. On the **Accounts** tab, specify one or more accounts for Configuration Manager to use when it connects to the target computer. Select the **Create** icon, enter the **User name** and **Password** (no more than 38 characters), confirm the password, and then select **OK**. Specify at least one client push installation account. This account must have local administrator rights on the target computer to install the client. If you don't specify a client push installation account, Configuration Manager tries to use the site system computer account. Cross-domain client push fails when using the site system computer account.

   > **NOTE**
   >
   > To use client push from a secondary site, specify the account at the secondary site that initiates the client push.
   >
   > For more information about the client push installation account, see the next procedure, Use the Client Push Installation Wizard.

8. Specify any required installation properties on the **Installation Properties** tab.

   If you've extended the Active Directory schema for Configuration Manager, the site publishes the specified client installation properties to Active Directory Domain Services. When CCMSetup runs without installation properties, it reads these properties from Active Directory.

   > **NOTE**
   >
   > If you enable client push installation on a secondary site, set the **SMSSITECODE** property to the Configuration Manager site code of its parent primary site. If you've extended the Active Directory schema for Configuration Manager, to automatically find the correct site assignment, set this property to **AUTO**.

Use the Client Push Installation Wizard

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**,

and select the **Sites** node.

2. Select the site for which you want to configure automatic site-wide client push installation.
3. On the **Home** tab of the ribbon, in the **Settings** group, select **Client Installation Settings**, and then select **Client Push Installation**.
4. Specify any required installation properties on the **Installation Properties** tab.

   If you've extended the Active Directory schema for Configuration Manager, the site publishes the specified client installation properties to Active Directory Domain Services. When CCMSetup runs without installation properties, it reads these properties from Active Directory.
5. In the Configuration Manager console, go to the **Assets and Compliance** workspace.
6. In the **Devices** node, select one or more computers. Or select a collection of computers in the **Device Collections** node.
7. On the **Home** tab of the ribbon, choose one of these options:
   - To push the client to one or more devices, in the **Device** group, select **Install Client**.
   - To push the client to a collection of devices, in the **Collection** group, select **Install Client**.
8. On the **Before You Begin** page of the Install Configuration Manager Client Wizard, review the information, and then select **Next**.
9. Select the appropriate options on the **Installation Options** page.
10. Review the installation settings, and then complete the wizard.

> **NOTE**
> Use this wizard to install clients even if the site isn't configured for client push.

Software update-based installation

Software update-based client installation publishes the client to a software update point as a software update. Use this method for a first-time installation or upgrade.

If the Configuration Manager client is installed on a computer, the computer receives client policy from the site. This policy includes the software update-point server name and port from which to get software updates.

> **IMPORTANT**
> For software update-based installation, use the same Windows Server Update Services (WSUS) server for client installation and software updates. This server must be the active software update point in a primary site. For more information, see Install a software update point.

If the Configuration Manager client isn't installed on a computer, configure and assign a Group Policy Object. The Group Policy specifies the server name of the software update point.

You can't add command-line properties to a software update-based client installation. If you've extended the Active Directory schema for Configuration Manager, the client installation automatically queries Active Directory Domain Services for the installation properties.

If you haven't extended the Active Directory schema, use Group Policy to provision client installation settings. These settings are automatically applied to any software update-based client installation. For more information,

see the section on How to provision client installation properties and the article on How to assign clients to a site.

Use the following procedures to configure computers without a Configuration Manager client to use the software update point. There's also a procedure for publishing the client software to the software update point.

> **TIP**
> If computers are in a pending restart state following a previous software installation, a software update-based client installation might cause the computer to restart.

Configure a Group Policy Object to specify the software update point

1. Use the **Group Policy Management Console** to open a new or existing Group Policy Object.
2. Expand **Computer Configuration**, **Administrative Templates**, and **Windows Components**, and then select **Windows Update**.
3. Open the properties of the setting **Specify intranet Microsoft update service location**, and then select **Enabled**.
4. **Set the intranet update service for detecting updates**: Specify the name and port of the software update point server.
   - If you've configured the Configuration Manager site system to use a fully qualified domain name (FQDN), use that format.
   - If the Configuration Manager site system isn't configured to use an FQDN, use a short name format.

   > **TIP**
   > To determine the port number, see How to determine the port settings used by WSUS.

   Example in the FQDN format: `http://server1.contoso.com:8530`
5. **Set the intranet statistics server**: This setting is typically configured with the same server name.
6. Assign the Group Policy Object to the computers on which you want to install the client and receive software updates.

Publish the Configuration Manager client to the software update point

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. Select the site for which you want to configure software update-based client installation.
3. On the **Home** tab of the ribbon, in the **Settings** group, select **Client Installation Settings**, and then select **Software Update-Based Client Installation**.
4. Select **Enable software update-based client installation**.
5. If the site's client version is more recent than the version on the software update point, the **Later Version of Client Package Detected** dialog box opens. Select **Yes** to publish the most recent version.

   > **NOTE**
   > If you haven't already published the client software to the software update point, this dialog box is blank.

The software update for the Configuration Manager client isn't automatically updated when there's a new version.

When you update the site, repeat this procedure to update the client.

Group Policy installation

Use Group Policy in Active Directory Domain Services to publish or assign the Configuration Manager client. The client installs when the computer starts. When you use Group Policy, the client appears in **Add or Remove Programs** in Control Panel. The user can install it from there.

Use the Windows Installer package CCMSetup.msi for Group Policy-based installations. This file is found in the `<ConfigMgr installation directory>\bin\i386` folder on the site server. You can't add properties to this file to change installation behavior.

> **IMPORTANT**
> You must have administrator permissions to access the client installation files.

- If you've extended the Active Directory schema for Configuration Manager, and you selected **Publish this site in Active Directory Domain Services** on the **Advanced** tab of the **Site Properties** dialog box, client computers automatically search Active Directory Domain Services for installation properties. For more information, see About client installation properties published to Active Directory Domain Services.
- If you haven't extended the Active Directory schema, see the section on provisioning client installation properties for information about storing installation properties in the Windows registry of computers. The client uses these installation properties when it installs.

For more information, see How to use Group Policy to remotely install software.

Manual installation

Manually install the client software on computers by using CCMSetup.exe. You can find this program and its supporting files in the Client folder in the Configuration Manager installation folder on the site server. The site shares this folder to the network as:

```
\\<site server name>\SMS_<site code>\Client\
```

`<site server name>` is the primary site server name. `<site code>` is the primary site code to which the client is assigned. To run CCMSetup.exe from the command line on the client, connect to this network location, and then run the command.

> **IMPORTANT**
> You must have administrator permissions to access the client installation files.

CCMSetup.exe copies all necessary prerequisites to the client computer and calls the Windows Installer package (Client.msi) to install the client. You can't run Client.msi directly.

To modify the behavior of the client installation, specify command-line options for both CCMSetup.exe and Client.msi. Make sure that you specify CCMSetup parameters that begin with `/` before you specify Client.msi properties. For example:

```
CCMSetup.exe /mp:SMSMP01 /logon SMSSITECODE=AUTO FSP=SMSFP01
```

In this example, the client installs with the following options:

OPTION	DESCRIPTION
`/mp:SMSMP01`	This CCMSetup parameter specifies the management point SMSMP01 for downloading the required client installation files.
`/logon`	This CCMSetup parameter specifies that the installation should stop if an existing Configuration Manager client is found on the computer.
`SMSSITECODE=AUTO`	This Client.msi property specifies that the client tries to locate the Configuration Manager site code to use, by using Active Directory Domain Services, for example.
`FSP=SMSFP01`	This Client.msi property specifies that the fallback status point named SMSFP01 is used to receive state messages sent from the client computer.

For more information, see About client installation parameters and properties.

> **TIP**
> For the procedure to install the Configuration Manager client on a modern Windows 10 device by using Azure Active Directory (Azure AD) identity, see Install and assign Configuration Manager Windows 10 clients using Azure AD for authentication. That procedure is for clients on an intranet or the internet.

Manual installation examples

These examples are for Active Directory-joined clients on an intranet. They use the following values:

- **MPSERVER**: server hosting the management point
- **FSPSERVER**: server hosting the fallback status point
- **ABC**: site code
- **contoso.com**: domain name

Assume that you've configured all site system servers with an intranet FQDN and published the site information to Active Directory.

Start with the following steps on the client computer:

1. Sign in as a local administrator.
2. Map drive Z to `\\MPSERVER\SMS_ABC\Client`.
3. Switch the command prompt to drive Z.

Then run one of the following commands:

Manual example 1

```
CCMSetup.exe
```

This command installs the client with no additional parameters or properties. The client is automatically configured with the client installation properties published to Active Directory Domain Services, including these settings:

- Site code: This setting requires the client's network location to be included in a boundary group that you've configured for client assignment.
- Management point.
- Fallback status point.

- Communicate using HTTPS only.

For more information, see About client installation properties published to Active Directory Domain Services.

Manual example 2

```
CCMSetup.exe /MP:mpserver.contoso.com /UsePKICert SMSSITECODE=ABC CCMHOSTNAME=server05.contoso.com
CCMFIRSTCERT=1 FSP=server06.constoso.com
```

This command overrides the automatic configuration that Active Directory Domain Services provides. It doesn't require that you include the client's network location in a boundary group that's configured for client assignment. Instead, the installation specifies these settings:

- Site code
- Intranet management point
- Internet-based management point
- Fallback status point that accepts connections from the internet
- Use a client public key infrastructure (PKI) certificate (if available) that has the longest validity period

Logon script installation

Configuration Manager supports using logon scripts to install the Configuration Manager client software. Use the program file CCMSetup.exe in a logon script to trigger the client installation.

Logon script installation uses the same methods as manual client installation. Specify the `/logon` installation parameter for CCMSsetup.exe. If any version of the client already exists on the computer, this parameter prevents the client from installing. This behavior prevents reinstallation of the client each time the logon script runs.

If you don't specify an installation source by using the `/Source` parameter and no management point from which to obtain installation is specified by the `/MP` parameter, CCMSetup.exe locates the management point by searching Active Directory Domain Services. This behavior occurs only if you've extended the schema for Configuration Manager and published the site to Active Directory Domain Services. Alternatively, the client can use DNS or WINS to locate a management point.

Package and program installation

Use Configuration Manager to create and deploy a package and program that upgrades the client software for selected devices. Configuration Manager supplies a package definition file that populates the package properties with typically used values. Customize the behavior of the client installation by specifying additional command-line parameters and properties.

> **NOTE**
>
> You can't upgrade Configuration Manager 2007 clients by using this method. Instead, use automatic client upgrade, which automatically creates and deploys a package that contains the latest version of the client. For more information, see Upgrade clients.
>
> For more information about how to migrate from older versions of the Configuration Manager client, see Planning a client migration strategy.

Create a package and program for the client software

Use the following procedure to create a Configuration Manager package and program that you can deploy to Configuration Manager client computers to upgrade the client software.

1. In the Configuration Manager console, go to the **Software Library** workspace, expand **Application Management**, and select the **Packages** node.

2. On the **Home** tab of the ribbon, in the **Create** group, select **Create Package from Definition**.
3. On the **Package Definition** page of the wizard, select **Microsoft** from the **Publisher** list, and select **Configuration Manager Client Upgrade** from the **Package definition** list.
4. On the **Source Files** page, select **Always obtain files from a source folder**.
5. On the **Source Folder** page, select **Network path (UNC Name)**. Then enter the network path of the server and share that contains the client installation files.

   > **NOTE**
   > The computer on which the Configuration Manager deployment runs must have access to the specified network folder. Otherwise, the client installation fails.

   To change any of the client installation properties, modify the CCMSetup.exe command line on the **General** tab of the **Configuration Manager agent silent upgrade Properties** program dialog box. The default installation properties are `/noservice SMSSITECODE=AUTO`.
6. Distribute the package to all distribution points that you want to host the client upgrade package. Then deploy the package to device collections that contain clients that you want to upgrade.

Intune MDM-managed Windows devices

Deploy the Configuration Manager client to devices that are enrolled with Microsoft Intune.

This procedure is for a traditional client that's connected to an intranet. It uses traditional client authentication methods. To make sure the device remains in a managed state after it installs the client, it must be on the intranet and within a Configuration Manager site boundary.

For the procedure to install the Configuration Manager client on a modern Windows 10 device by using Azure AD identity, see Install and assign Configuration Manager Windows 10 clients using Azure AD for authentication.

After you install the Configuration Manager client, devices don't unenroll from Intune. They can use the Configuration Manager client and MDM enrollment at the same time. For more information, see Co-management overview.

> **NOTE**
> You can use other client installation methods to install the Configuration Manager client on an Intune-managed device. For example, if an Intune-managed device is on the intranet, and joined to the Active Directory domain, you can use group policy to install the Configuration Manager client.

Install the Configuration Manager client by using Intune

1. In Intune, add a Windows line-of-business app that contains the Configuration Manager client installation file **CCMSetup.msi**. You can find this file in the `\bin\i386` folder of the Configuration Manager installation directory on the site server.
2. In the Intune Software Publisher, enter command-line parameters. For example, use this command with a traditional client on an intranet:

```
CCMSETUPCMD="/MP:<FQDN of management point> SMSMP=<FQDN of management point> SMSSITECODE=<your site
code> DNSSUFFIX=<DNS suffix of management point>"
```

> **NOTE**
> For an example of a command to use with a modern Windows 10 client using Azure AD authentication, see How to prepare internet-based devices for co-management.

3. Assign the app to a group of the enrolled Windows computers.

OS image installation

Preinstall the Configuration Manager client on a reference computer that you use to create an OS image.

> **IMPORTANT**
> When you use the Configuration Manager task sequence to deploy an OS image, the Prepare ConfigMgr Client step completely removes the Configuration Manager client.

Prepare the client computer for imaging

1. Manually install the Configuration Manager client software on the reference computer. For more information, see How to install Configuration Manager clients manually.

   > **IMPORTANT**
   > Don't specify a Configuration Manager site code for the client in the CCMSetup.exe command-line properties.

2. At a command prompt, type `net stop ccmexec` to stop the SMS Agent Host service (CcmExec.exe) on the reference computer.
3. Delete the SMSCFG.INI file from the Windows folder on the reference computer.
4. Remove any certificates that are stored in the local computer store on the reference computer. For example, if you use PKI certificates, before you image the computer, remove the certificates in the **Personal** store for **Computer** and **User**.
5. If the clients are installed in a different Configuration Manager hierarchy than the hierarchy of the reference computer, remove the trusted root key from the reference computer.

   > **NOTE**
   > If clients can't query Active Directory Domain Services to locate a management point, they use the trusted root key to determine trusted management points. If you deploy all imaged clients in the same hierarchy as that of the master computer, leave the trusted root key in place.
   >
   > If you deploy the clients in different hierarchies, remove the trusted root key. Also provision these clients with the new trusted root key. For more information, see Planning for the trusted root key.

6. Use your imaging software to capture an image of the reference computer.
7. Deploy the image to the destination computers.

Workgroup computers

Configuration Manager supports client installation for computers in workgroups. Install the client on workgroup computers by using the method specified in How to install Configuration Manager clients manually.

Prerequisites

- Manually install the client on each workgroup computer. During installation, the interactive user must have local administrator rights.
- To access resources in the Configuration Manager site server domain, configure the network access account for the site. Specify this account in the software distribution site component. For more information, see Site components.

Limitations

- Workgroup clients can't locate management points from Active Directory Domain Services. Instead, they use DNS, WINS, or another management point.
- Global roaming isn't supported. Workgroup clients can't query Active Directory Domain Services for site information.
- Active Directory discovery methods can't discover computers in workgroups.
- You can't deploy software to users of workgroup computers.
- You can't use the client push installation method to install the client on workgroup computers.
- Workgroup clients can't use Kerberos for authentication, and they might require manual approval.
- You can't configure a workgroup client as a distribution point. Configuration Manager requires that distribution point computers be members of a domain.

Install the client on workgroup computers

Check the prerequisites, and then follow the directions in the section How to install Configuration Manager clients manually.

Workgroup example 1

This example does the following actions:

- Installs the client for intranet client management
- Specifies the site code
- Specifies the DNS suffix to locate a management point

```
CCMSetup.exe SMSSITECODE=ABC DNSSUFFIX=constoso.com
```

Workgroup example 2

This example requires the client to be on a network location that's configured in a boundary group. If this requirement isn't met, automatic site assignment won't work. The command includes a fallback status point on server FSPSERVER. This property helps to track client deployment and to identify any client communication issues.

```
CCMSetup.exe FSP=fspserver.constoso.com
```

Internet-based client management

> **NOTE**
> This section doesn't apply to clients that use a cloud management gateway. To install internet-based clients by using a cloud management gateway, see Install and assign Configuration Manager Windows 10 clients using Azure AD for authentication.

When the Configuration Manager site supports internet-based client management for clients that are sometimes on an intranet and sometimes on the internet, you have two options when you install clients on the intranet:

- Include the Client.msi property `CCMHOSTNAME=<internet FQDN of the internet-based management point>` when you install the client, by using manual installation or client push, for example. When you use this method, directly assign the client to the site. You can't use automatic site assignment. See the How to install Configuration Manager clients manually section, which provides an example of this configuration method.
- Install the client for intranet client management, and then assign an internet-based client management point to the client. Change the management point by using the client properties on the **Configuration Manager** page in Control Panel, or by using a script. When you use this method, you can use automatic client assignment. For more information, see the How to configure clients for internet-based client management after client installation section.

To install clients that are on the internet, choose one of the following supported methods:

- Provide a mechanism for these clients to temporarily connect to the intranet with a VPN. Then install the client by using any appropriate client installation method.
- Use an installation method that's independent of Configuration Manager. For example, package the client installation source files onto removable media and send the media to users. The client installation source files are located in the `<installation path>\Client` folder on the Configuration Manager site server. On the media, include a script to manually copy over the client folder. From this folder, install the client by using CCMSetup.exe and all the appropriate CCMSetup command-line properties.

> **NOTE**
> Configuration Manager doesn't support installing a client directly from the internet-based management point or from the internet-based software update point.

Clients that are managed over the internet must communicate with internet-based site systems. Ensure that these clients also have public key infrastructure (PKI) certificates before you install the client. Install these certificates independently from Configuration Manager. For more information, see PKI certificate requirements.

Install clients on the internet by specifying CCMSetup command-line properties

1. Follow the directions in the section How to install Configuration Manager clients manually. Always include the following options:
   - CCMSetup command-line parameter `/source:<local path of the copied Client folder>`
   - CCMSetup command-line parameter `/UsePKICert`
   - Client.msi property `CCMHOSTNAME=<FQDN of internet-based management point>`
   - Client.msi property `SMSSIGNCERT=<local path of exported site server signing certificate>`
   - Client.msi property `SMSSITECODE=<site code of internet-based management point>`

   > **NOTE**
   > If the site has more than one internet-based management point, it doesn't matter which one you specify for the `CCMHOSTNAME` property. When a Configuration Manager client connects to the specified internet-based management point, it sends the client a list of available internet-based management points in the site. The client randomly selects one from the list.

2. If you don't want the client to check the certificate revocation list (CRL), specify the CCMSetup command-line parameter `/NoCRLCheck`.
3. If you're using an internet-based fallback status point, specify the Client.msi property

`FSP=<internet FQDN of the internet-based fallback status point>`.

4. If you're installing the client for internet-only client management, specify the Client.msi property `CCMALWAYSINF=1`.

5. Determine whether you have to specify additional CCMSetup command-line parameters. For example, if the client has more than one valid PKI certificate, you might have to specify a certificate selection criterion. For a list of available properties, see About client installation parameters and properties.

Internet-based example

```
CCMSetup.exe /source: D:\Clients /UsePKICert CCMHOSTNAME=server1.contoso.com SMSSIGNCERT=siteserver.cer
SMSSITECODE=ABC FSP=server2.contoso.com CCMALWAYSINF=1 CCMFIRSTCERT=1
```

This example installs the client with the following behaviors:

- Use source files from a folder on drive D.
- Use a client PKI certificate.
- Select the certificate with the longest validity period.
- Internet-only client management.
- Assign the client to use the internet-based management point named SERVER1.
- Assign the internet-based fallback status point in the contoso.com domain.
- Assign the client to the ABC site.

To configure clients for internet-based client management after client installation

To assign the internet-based management point after you install the client, use one of these procedures. The first requires manual configuration and is appropriate for a few clients. The second is more appropriate for configuring many clients.

Configure clients for internet-based client management after client installation from the Configuration Manager control panel

1. Open the **Configuration Manager** control panel on the client.

2. On the **Internet** tab, enter the fully qualified domain name (FQDN) of the internet-based management point as the **Internet FQDN**.

> **NOTE**
>
> The **Internet** tab is available only if the client has a client PKI certificate.

3. If the client accesses the internet by using a proxy server, enter the proxy server settings.

Configure clients for internet-based client management after client installation by using a script

PowerShell

1. Open a PowerShell in-line editor, like PowerShell ISE or Visual Studio Code. You can also use a text editor, like Notepad.

2. Copy and insert the following lines of code into the editor. Replace `'mp.contoso.com'` with the internet FQDN of your internet-based management point.

```
$newInternetBasedManagementPointFQDN = 'mp.contoso.com'
$client = New-Object -ComObject Microsoft.SMS.Client
$client.SetInternetManagementPointFQDN($newInternetBasedManagementPointFQDN)
Restart-Service CcmExec
$client.GetInternetManagementPointFQDN()
```

> **NOTE**
> The last line is there only to verify the new internet management point value.
>
> To delete a specified internet-based management point, remove the server FQDN value inside the quotation marks. The line becomes `$newInternetBasedManagementPointFQDN = ''`.

3. Save the file with a .ps1 extension.
4. Run the script with elevated rights on client computers. Use one of these methods:
   - Deploy the file to existing Configuration Manager clients by using a package and a program.
   - Run the file locally on existing Configuration Manager clients by double-clicking the script file in File Explorer.

You might have to restart the client for the changes to take effect.

Provision client installation properties

Provision client installation properties for group policy and software update-based client installations. Use Windows Group Policy to provision computers with Configuration Manager client installation properties. These properties are stored in the registry of the computer. The client reads them when it installs. This procedure isn't normally required, but it might be needed for some client installation scenarios, such as:

- You're using the group policy settings or software update-based client installation methods. You haven't extended the Active Directory schema for Configuration Manager.
- You want to override client installation properties on specific computers.

> **NOTE**
> If any installation properties are supplied on the CCMSetup.exe command line, installation properties provisioned on computers aren't used.

A group policy administrative template named `ConfigMgrInstallation.adm` is supplied on the Configuration Manager installation media. Use this template to provision client computers with installation properties.

> **TIP**
> By default, `ConfigMgrInstallation.adm` doesn't support strings larger than 255 characters. This configuration can impact adding multiple parameters or parameters with long values, such as CCMCERTISSUERS.
>
> To workaround this issue:
>
> 1. Edit `ConfigMgrInstallation.adm` in Notepad.
> 2. For the property `VALUENAME SetupParameters`, change the `MAXLEN` value to a larger integer. For example, `MAXLEN 511`.

Configure and assign client installation properties by using a group policy object

1. Import the ConfigMgrInstallation.adm administrative template into a new or existing group policy object (GPO) by using an editor like Windows Group Policy Object Editor. You can find this file in the `TOOLS\ConfigMgrADMTemplates` folder on the Configuration Manager installation media.
2. Open the properties of the imported setting **Configure Client Deployment Settings**.

3. Select **Enabled**.
4. In the **CCMSetup** box, enter the required CCMSetup command-line properties. For a list of all CCMSetup command-line properties and examples of their use, see About client installation parameters and properties.
5. Assign the GPO to the computers that you want to provision with Configuration Manager client installation properties.

Install and assign Configuration Manager Windows 10 clients using Azure AD for authentication

7/9/2019 • 4 minutes to read • Edit Online

To install the Configuration Manager client on Windows 10 devices using Azure AD authentication, integrate Configuration Manager with Azure Active Directory (Azure AD). Clients can be on the intranet communicating directly with an HTTPS-enabled management point or any management point in a site enabled for Enhanced HTTP. They can also be internet-based communicating through the CMG or with an Internet-based management point. This process uses Azure AD to authenticate clients to the Configuration Manager site. Azure AD replaces the need to configure and use client authentication certificates.

Setting up Azure AD may be easier for some customers than setting up a public key infrastructure for certificate-based authentication. There are features that require you onboard the site to Azure AD, but don't necessarily require the clients to be Azure AD-joined. For more information, see the following articles:

- Plan for Azure Active Directory
- Use Azure AD for co-management

Before you begin

- An Azure AD tenant is a prerequisite
- Device requirements:
  - Windows 10
  - Joined to Azure AD, either pure cloud domain-joined, or hybrid Azure AD-joined
- User requirements:
  - The logged on user must be an Azure AD identity.
  - If the user is a federated or synchronized identity, you must use Configuration Manager Active Directory user discovery as well as Azure AD user discovery. For more information about hybrid identities, see Define a hybrid identity adoption strategy.
- In addition to the existing prerequisites for the management point site system role, also enable **ASP.NET 4.5** on this server. Include any other options that are automatically selected when enabling ASP.NET 4.5.
- Determine whether your management point needs HTTPS. For more information, see Enable management point for HTTPS.
- Optionally set up a cloud management gateway (CMG) to deploy internet-based clients. For on-premises clients that authenticate with Azure AD, you don't need a CMG.

Configure Azure Services for Cloud Management

Connect your Configuration Manager site to Azure AD as the first step. For details of this process, see Configure Azure services. Create a connection to the **Cloud Management** service.

Enable Azure AD User Discovery as part of onboarding to **Cloud Management**.

After you complete these actions, your Configuration Manager site is connected to Azure AD.

Configure client settings

These client settings help join Windows 10 devices with Azure AD. They also enable internet-based clients to use the CMG and cloud distribution point.

1. Configure the following client settings in the **Cloud Services** section using the information in How to configure client settings.

   - **Allow access to cloud distribution point**: Enable this setting to help internet-based devices get the required content to install the Configuration Manager client. If the content isn't available on the cloud distribution point, devices can retrieve the content from the CMG. The client installation bootstrap retries the cloud distribution point for four hours before it falls back to the CMG.
   - **Automatically register new Windows 10 domain joined devices with Azure Active Directory**: Set to **Yes** or **No**. The default setting is **Yes**. This behavior is also the default in Windows 10, version 1709.
   - **Enable clients to use a cloud management gateway** – Set to **Yes** (default), or **No**.

2. Deploy the client settings to the required collection of devices. Do not deploy these settings to user collections.

To confirm the device is joined to Azure AD, run `dsregcmd.exe /status` in a command prompt. The **AzureAdjoined** field in the results shows **YES** if the device is Azure AD-joined.

Install and register the client using Azure AD identity

To manually install the client using Azure AD identity, first review the general process on How to install clients manually.

> **NOTE**
> The device needs access to the internet to contact Azure AD, but doesn't need to be internet-based.

The following example shows the general structure of the command line:

```
ccmsetup.exe /mp:<source management point> CCMHOSTNAME=<internet-based management point> SMSSiteCode=<site code>
SMSMP=<initial management point> AADTENANTID=<Azure AD tenant identifier> AADCLIENTAPPID=<Azure AD client app
identifier> AADRESOURCEURI=<Azure AD server app identifier>
```

For more information, see Client installation properties.

The /mp and CCMHOSTNAME properties specify one of the following, depending upon the scenario:

- On-premises management point. Only specify the /mp property. The CCMHOSTNAME isn't required.
- Cloud management gateway
- Internet-based management point The SMSMP property specifies either the on-premises or internet-based management point.

This example uses a cloud management gateway. It substitutes sample values for each property:

```
ccmsetup.exe /mp:https://CONTOSO.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72186325152220500
CCMHOSTNAME=CONTOSO.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72186325152220500 SMSSiteCode=ABC
SMSMP=https://mp1.contoso.com AADTENANTID=daf4a1c2-3a0c-401b-966f-0b855d3abd1a AADCLIENTAPPID=7506ee10-f7ec-
415a-b415-cd3d58790d97 AADRESOURCEURI=https://contososerver
```

Starting in version 1810, the site publishes additional Azure AD information to the cloud management gateway (CMG). An Azure AD-joined client gets this information from the CMG during the ccmsetup process, using the same tenant to which it's joined. This behavior further simplifies installing the client in an environment with more than one Azure AD tenant. Now the only two required ccmsetup properties are **CCMHOSTNAME** and

SMSSiteCode.

To automate the client install using Azure AD identity via Microsoft Intune, see How to prepare internet-based devices for co-management.

Next steps

Once complete, you can continue to monitor and manage clients.

About client installation parameters and properties in System Center Configuration Manager

8/30/2019 • 23 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the CCMSetup.exe command to install the Configuration Manager client. If you provide client installation parameters on the command line, they modify the installation behavior. If you provide client installation properties on the command-line, they modify the initial configuration of the installed client agent.

About CCMSetup.exe

The CCMSetup.exe command downloads needed files to install the client from a management point or a source location. These files might include:

- The Windows Installer package client.msi that installs the client software.
- Microsoft Background Intelligent Transfer Service (BITS) installation files.
- Windows Installer installation files.
- Updates and fixes for the Configuration Manager client.

> **NOTE**
> In Configuration Manager, you can't run the Client.msi file directly.

CCMSetup.exe provides command-line parameters to customize the installation -- parameters are prefixed with a backslash and by convention are lower case. You specify the value of a parameter when necessary using a colon immediately followed by the desired value. You can also supply properties to modify the behavior of client.msi at the CCMSetup.exe command line -- properties by convention are in all upper case. You specify a value for a property using an equal sign immediately followed by the desired value.

> **IMPORTANT**
> Specify CCMSetup parameters before you specify properties for client.msi.

CCMSetup.exe and the supporting files are located on the site server in the **Client** folder of the Configuration Manager installation folder. This folder is shared to the network as **<Site Server Name>\SMS_<Site Code>\Client**.

At the command prompt, the CCMSetup.exe command uses the following format:

```
CCMSetup.exe [<Ccmsetup parameters>] [<client.msi setup properties>]
```

For example:

```
CCMSetup.exe /mp:SMSMP01 /logon SMSSITECODE=S01 FSP=SMSFSP01
```

This example does the following things:

- Specifies the management point named SMSMP01 to request a list of distribution points to download the

client installation files.

- Specifies that installation should stop if a version of the client already exists on the computer.
- Instructs client.msi to assign the client to the site code S01.
- Instructs client.msi to use the fallback status point named SMSFP01.

> **NOTE**
> If a parameter value has spaces, surround it with quotation marks.

> **IMPORTANT**
> If you extended the Active Directory schema for Configuration Manager, the site publishes many client installation properties in Active Directory Domain Services. The Configuration Manager client automatically reads these properties. For more information, see About client installation properties published to Active Directory Domain Services

CCMSetup.exe command-line parameters

/?

Opens the **CCMSetup** dialog box showing command-line parameters for ccmsetup.exe.

Example: **ccmsetup.exe /?**

/source:<Path>

Specifies the file download location. Use a local or UNC path. Files are downloaded using the server message block (SMB) protocol. To use **/source**, the Windows user account for client installation must have Read permissions to the location.

> **NOTE**
> You can use the **/source** parameter more than once in a command line to specify alternative download locations.

Example: **ccmsetup.exe /source:"\\computer\folder"**

/mp:<Server>

Specifies a source management point for computers to connect to. Computers use this management point to find the nearest distribution point for the installation files. If there are no distribution points, or computers can't download the files from the distribution points after four hours, they download the files from the specified management point.

> **IMPORTANT**
> This parameter is used to specify an initial management point for computers to find a download source, and can be any management point in any site. It doesn't *assign* the client to a management point.

Computers download the files over an HTTP or HTTPS connection, depending on the site system role configuration for client connections. If configured, the download uses BITS throttling. If all distribution points and management points are configured for HTTPS client connections only, verify that the client computer has a valid client certificate.

You can use the **/mp** command-line parameter to specify more than one management point. If the computer fails

to connect to the first one, it tries the next in the specified list. When you specify multiple management points, separate the values by semicolons.

If the client connects to a management point using HTTPS, typically, you must specify the FQDN, not the computer name. The value must match the management point's PKI certificate Subject or Subject Alternative Name. Although Configuration Manager supports using a computer name in the certificate for connections on the intranet, using an FQDN is recommended.

Example for when you use the computer name: `ccmsetup.exe /mp:SMSMP01`

Example for when you use the FQDN: `ccmsetup.exe /mp:smsmp01.contoso.com`

This parameter can specify the URL of a cloud management gateway. Use this URL to install the client on an internet-based device. To get the value for this parameter, use the following steps:

- Create a cloud management gateway.
- On an active client, open a Windows PowerShell command prompt as an administrator.
- Run the following command:
  ```
  (Get-WmiObject -Namespace Root\Ccm\LocationServices -Class SMS_ActiveMPCandidate | Where-Object {$_.Type -eq "Internet"}).MP
  ```
- Append the "https://" prefix to use with the **/mp** parameter.

Example for when you use the cloud management gateway URL:
`ccmsetup.exe /mp:https://CONTOSO.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72057598037248100`

> **IMPORTANT**
> When specifying the URL of a cloud management gateway for the **/mp** parameter, it must start with **https://**.

/retry:<Minutes>

The retry interval if CCMSetup.exe fails to download installation files. CCMSetup continues to retry until it reaches the limit specified in the **downloadtimeout** parameter.

Example: `ccmsetup.exe /retry:20`

/noservice

Prevents CCMSetup from running as a service, which is the default. When CCMSetup runs as a service, it runs in the context of the Local System account of the computer. This account might not have sufficient rights to access required network resources for the installation. With **/noservice**, CCMSetup.exe runs in the context of the user account that you use to start the installation. Also, if you're using a script to run CCMSetup.exe with the **/service** parameter, CCMSetup.exe exits after the service starts and might not report installation details correctly.

Example: `ccmsetup.exe /noservice`

/service

Specifies that CCMSetup should run as a service that uses the local system account.

Example: `ccmsetup.exe /service`

/uninstall

Specifies that the client software should be uninstalled. For more information, see How to manage clients.

Example: `ccmsetup.exe /uninstall`

/logon

If any version of the client is already installed, this parameter specifies that the client installation should stop.

Example: `ccmsetup.exe /logon`

/forcereboot

Specifies that CCMSetup should force the client computer to restart if necessary to complete the installation. If this parameter isn't specified, CCMSetup exits when a restart is necessary. It then continues after the next manual restart.

Example: `CCMSetup.exe /forcereboot`

/BITSPriority:<Priority>

Specifies the download priority when client installation files are downloaded over an HTTP connection. Possible values are as follows:

- FOREGROUND
- HIGH
- NORMAL
- LOW

  The default value is NORMAL.

  Example: `ccmsetup.exe /BITSPriority:HIGH`

/downloadtimeout:<Minutes>

The length of time in minutes that CCMSetup tries to download the installation files before stopping. The default value is **1440** minutes (one day).

Example: `ccmsetup.exe /downloadtimeout:100`

/UsePKICert

When specified, the client uses a PKI certificate that includes client authentication, if available. If the client can't find a valid certificate, it uses an HTTP connection with a self-signed certificate. This behavior is the same when you don't use this parameter.

> **NOTE**
> In some scenarios, you do not have to specify this parameter when you are installing a client, and still use a client certificate. These scenarios include installing a client by using client push, and software update point–based client installation. However, you must specify this parameter whenever you manually install a client and use the **/mp** parameter to specify a management point that is configured to accept only HTTPS client connections. You also must specify this parameter when you install a client for internet-only communication. Use the CCMALWAYSINF=1 property together with the properties for the internet-based management point (CCMHOSTNAME) and the site code (SMSSITECODE). For more information about internet-based client management, see Considerations for client communications from the internet or an untrusted forest.

Example: `CCMSetup.exe /UsePKICert`

/NoCRLCheck

Specifies that a client shouldn't check the certificate revocation list (CRL) when it communicates over HTTPS with a PKI certificate.

When not specified, the client checks the CRL before establishing an HTTPS connection.

For more information about client CRL checking, see Planning for PKI certificate revocation.

Example: `CCMSetup.exe /UsePKICert /NoCRLCheck`

/config:<configuration file>

Specifies the name of a text file that lists client installation properties.

- If you don't specify the **/noservice** CCMSetup parameter, this file must be located in the CCMSetup folder, which is %Windir%\Ccmsetup for 32-bit and 64-bit operating systems.
- If you specify the **/noservice** parameter, this file must be located in the same folder from which you run CCMSetup.exe.

Example: `CCMSetup.exe /config:<Configuration File Name.txt\>`

To provide the correct file format, use the mobileclienttemplate.tcf file in the <Configuration Manager directory>\bin\<platform> folder on the site server. This file also has comments about the sections and how they're used. Specify the client installation properties in the [Client Install] section, after the following text: **Install=INSTALL=ALL**.

Example [Client Install] section entry: `Install=INSTALL=ALL SMSSITECODE=ABC SMSCACHESIZE=100`

/skipprereq:<filename>

Specifies that CCMSetup.exe must not install the specified prerequisite program when installing the Configuration Manager client. This parameter supports entering more than one value. Use the semicolon character (;) to separate each value.

Examples: `CCMSetup.exe /skipprereq:dotnetfx40_client_x86_x64.exe` or `CCMSetup.exe /skipprereq:dotnetfx40_client_x86_x64.exe;windowsupdateagent30_x86.exe`

/forceinstall

Specify that CCMSetup.exe uninstalls any existing client, and installs a new client.

/ExcludeFeatures:<feature>

Specifies that CCMSetup.exe doesn't install the specified feature when it installs the client.

Example: `CCMSetup.exe /ExcludeFeatures:ClientUI` doesn't install Software Center on the client.

> **NOTE**
>
> **ClientUI** is the only value supported with the **/ExcludeFeatures** parameter.

CCMSetup.exe return codes

The CCMSetup.exe command provides the following return codes completed. To troubleshoot, review the ccmsetup.log file on the client computer for context and additional detail about return codes.

RETURN CODE	MEANING
0	Success
6	Error
7	Reboot required
8	Setup already running
9	Prerequisite evaluation failure

RETURN CODE	MEANING
10	Setup manifest hash validation failure

Ccmsetup.msi properties

The following properties can modify the installation behavior of ccmsetup.msi.

CCMSETUPCMD

Specifies command-line parameters and properties that are passed to ccmsetup.exe after it is installed by ccmsetup.msi. Include other properties inside quotation marks. Use this property when bootstrapping the Configuration Manager client using the Intune MDM installation method.

Example: `ccmsetup.msi CCMSETUPCMD="/mp:https://mp.contoso.com CCMHOSTNAME=mp.contoso.com"`

> **TIP**
> Microsoft Intune limits the command line to 1024 characters.

Client.msi properties

The following properties can modify the installation behavior of client.msi. If you use the client push installation method, you can also specify the properties in the **Client** tab of the **Client Push Installation Properties** dialog box.

AADCLIENTAPPID

Specifies the Azure Active Directory (Azure AD) client app identifier. The client app is created or imported when you configure Azure services for Cloud Management. An Azure administrator can get the value for this property from the Azure portal. For more information, see get application ID. For the **AADCLIENTAPPID** property, this application ID is for the "Native" application type.

Example: `ccmsetup.exe AADCLIENTAPPID=aa28e7f1-b88a-43cd-a2e3-f88b257c863b`

AADRESOURCEURI

Specifies the Azure AD server app identifier. The server app is created or imported when you configure Azure services for Cloud Management. When creating the server app, in the Create Server Application dialog, this property is the **App ID URI**.

An Azure administrator can get the value for this property from the Azure portal. In the **Azure Active Directory** blade, find the server app under **App registrations**. This app is of "Web app / API" application type. Open the app, click **Settings**, and then **Properties**. Use the **App ID URI** value for this AADRESOURCEURI client installation property.

Example: `ccmsetup.exe AADRESOURCEURI=https://contososerver`

AADTENANTID

Specifies the Azure AD tenant identifier. This tenant is linked to Configuration Manager when you configure Azure services for Cloud Management. To obtain the value for this property, use the following steps:

- On a Windows 10 device that is joined to the same Azure AD tenant, open a command prompt.
- Run the following command: `dsregcmd.exe /status`
- In the Device State section, find the **TenantId** value. For example,
  `TenantId : 607b7853-6f6f-4d5d-b3d4-811c33fdd49a`

> **NOTE**
> An Azure administrator can also obtain this value in the Azure portal. For more information, see get tenant ID

Example: `ccmsetup.exe AADTENANTID=607b7853-6f6f-4d5d-b3d4-811c33fdd49a`

CCMADMINS

Specifies one or more Windows user accounts or groups to be given access to client settings and policies. This property is useful where the Configuration Manager admin doesn't have local administrative credentials on the client computer. Specify a list of accounts that are separated by semi-colons.

Example: `CCMSetup.exe CCMADMINS="Domain\Account1;Domain\Group1"`

CCMALLOWSILENTREBOOT

Specifies that the computer is allowed to restart following the client installation if necessary.

> **IMPORTANT**
> The computer restarts without warning even if a user is logged on.

Example: **CCMSetup.exe CCMALLOWSILENTREBOOT**

CCMALWAYSINF

Set to **1** to specify that the client is always internet-based and never connects to the intranet. The client's connection type displays **Always Internet**.

Use this property in conjunction with CCMHOSTNAME, which specifies the FQDN of the internet-based management point. Also use it with the CCMSetup parameter /UsePKICert, and with the site code.

For more information about internet-based client management, see Considerations for client communications from the internet or an untrusted forest.

Example: `CCMSetup.exe /UsePKICert CCMALWAYSINF=1 CCMHOSTNAME=SERVER3.CONTOSO.COM SMSSITECODE=ABC`

CCMCERTISSUERS

Specifies the certificate issuers list, which is a list of trusted root certification (CA) certificates that the Configuration Manager site trusts.

For more information about the certificate issuers list and how clients use it during the certificate selection process, see Planning for PKI client certificate selection.

This value is a case-sensitive match for subject attributes that are in the root CA certificate. Attributes can be separated by a comma (,) or semi-colon (;). Specify more than one root CA certificates by using a separator bar. Example:

```
CCMCERTISSUERS="CN=Contoso Root CA; OU=Servers; O=Contoso, Ltd; C=US | CN=Litware Corporate Root CA;
O=Litware, Inc."
```

> **TIP**
> To copy the **CertificateIssuers=<string>** for the site, reference the mobileclient.tcf file in the <Configuration Manager directory>\bin\<platform> folder on the site server.

CCMCERTSEL

Specifies the certificate selection criteria if the client has more than one certificate for HTTPS communication.

This certificate is a valid certificate that includes the client authentication capability.

You can search for an exact match (use **Subject:**) or a partial match (use **SubjectStr:)** in the Subject Name or Subject Alternative Name. Examples:

`CCMCERTSEL="Subject:computer1.contoso.com"` searches for a certificate with an exact match to the computer name "computer1.contoso.com" in the Subject Name or the Subject Alternative Name.

`CCMCERTSEL="SubjectStr:contoso.com"` searches for a certificate that contains "contoso.com" in the Subject Name or the Subject Alternative Name.

You can also use Object Identifier (OID) or distinguished name attributes in the Subject Name or Subject Alternative Name attributes, for example:

`CCMCERTSEL="SubjectAttr:2.5.4.11 = Computers"` searches for the organizational unit attribute expressed as an object identifier, and named Computers.

`CCMCERTSEL="SubjectAttr:OU = Computers"` searches for the organizational unit attribute expressed as a distinguished name, and named Computers.

> **IMPORTANT**
>
> If you use the Subject Name box, the **Subject:** is case-sensitive, and the **SubjectStr:** is case-insensitive.
>
> If you use the Subject Alternative Name box, the **Subject:**and the **SubjectStr:** are case-insensitive.

The complete list of attributes that you can use for certificate selection is listed in Supported attribute values for the PKI certificate selection criteria.

If more than one certificate matches the search, and the property CCMFIRSTCERT has been set to 1, the certificate with the longest validity period is selected.

CCMCERTSTORE

Specifies an alternate certificate store name if the client certificate for HTTPS isn't located in the default certificate store of **Personal** in the Computer store.

Example: `CCMSetup.exe /UsePKICert CCMCERTSTORE="ConfigMgr"`

CCMDEBUGLOGGING

Enables debug logging. Values can be set to 0 (off, default) or 1 (on). This property causes the client to log low-level information for troubleshooting. As a best practice, avoid using this property in production sites. Excessive logging can occur, which might make it difficult to find relevant information in the log files. Also set CCMENABLELOGGING to TRUE to enable debug logging.

Example: `CCMSetup.exe CCMDEBUGLOGGING=1`

CCMENABLELOGGING

By default, this property is set to TRUE to enable logging. The log files are stored in the **Logs** folder in the Configuration Manager client installation folder. By default, this folder is %Windir%\CCM\Logs.

Example: `CCMSetup.exe CCMENABLELOGGING=TRUE`

CCMEVALINTERVAL

The frequency at which client health evaluation tool (ccmeval.exe) runs. Can be **1** to **1440** minutes. By default, runs once a day.

CCMEVALHOUR

The hour when the client health evaluation tool (ccmeval.exe) runs, between **0** (midnight) and **23** (11pm). Runs at

midnight by default.

CCMFIRSTCERT

If set to 1, this property specifies that the client should select the PKI certificate with the longest validity period.

Example: `CCMSetup.exe /UsePKICert CCMFIRSTCERT=1`

CCMHOSTNAME

If the client is managed over the internet, this property specifies the FQDN of the internet-based management point.

Don't specify this option with the installation property of SMSSITECODE=AUTO. Internet-based clients must be directly assigned to their internet-based site.

Example: `CCMSetup.exe /UsePKICert CCMHOSTNAME="SMSMP01.corp.contoso.com"`

This property can specify the address of a cloud management gateway. To get the value for this property, use the following steps:

- Create a cloud management gateway.
- On an active client, open a Windows PowerShell command prompt as an administrator.
- Run the following command:
  ```
  (Get-WmiObject -Namespace Root\Ccm\LocationServices -Class SMS_ActiveMPCandidate | Where-Object {$_.Type -eq "Internet"}).MP
  ```
- Use the returned value as-is with the **CCMHOSTNAME** property.

For example: `ccmsetup.exe CCMHOSTNAME=CONTOSO.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72057598037248100`

> **IMPORTANT**
> When specifying the address of a cloud management gateway for the **CCMHOSTNAME** property, do *not* append a prefix such as **https://**. This prefix is only used with the **/mp** URL of a cloud management gateway.

CCMHTTPPORT

Specifies the port that the client should use when communicating over HTTP to site system servers. Set to Port 80 by default.

Example: `CCMSetup.exe CCMHTTPPORT=80`

CCMHTTPSPORT

Specifies the port that the client should use when communicating over HTTPS to site system servers. Set to Port 443 by default.

Example: `CCMSetup.exe /UsePKICert CCMHTTPSPORT=443`

CCMINSTALLDIR

Identifies the folder where the Configuration Manager client files are installed, *%Windir%*\CCM by default. Regardless of where these files are installed, the Ccmcore.dll file is always installed in the *%Windir%**System32* folder. Also, on a 64-bit OS, a copy of the Ccmcore.dll file is always installed in the *%Windir%*\SysWOW64 folder. This file supports 32-bit applications that use the 32-bit version of the client APIs from the Configuration Manager SDK.

Example: `CCMSetup.exe CCMINSTALLDIR="C:\ConfigMgr"`

CCMLOGLEVEL

Specifies the level of detail to write to Configuration Manager log files. Specify an integer from 0 to 3, where 0 is the most verbose logging and 3 logs only errors. The default is 1.

Example: `CCMSetup.exe CCMLOGLEVEL=3`

CCMLOGMAXHISTORY

When a Configuration Manager log file reaches the maximum size, the client renames it as a backup and creates a new log file. The maximum size is 250,000 bytes by default, or the value specified by the property CCMLOGMAXSIZE.

This property specifies how many previous versions of the log file to keep. The default value is 1. If the value is set to 0, no old log files are kept.

Example: `CCMSetup.exe CCMLOGMAXHISTORY=0`

CCMLOGMAXSIZE

The maximum log file size in bytes. When a log grows to the specified size, the client renames it as a history file, and creates a new file. This property must be set to at least 10,000 bytes. The default value is 250,000 bytes.

Example: `CCMSetup.exe CCMLOGMAXSIZE=300000`

DISABLESITEOPT

If set to TRUE, this property disables the ability of administrative users from changing the assigned site in the **Configuration Manager** control panel.

Example: **CCMSetup.exe DISABLESITEOPT=TRUE**

DISABLECACHEOPT

If set to TRUE, this property disables the ability of administrative users from changing the client cache folder settings in the **Configuration Manager** control panel.

Example: `CCMSetup.exe DISABLECACHEOPT=TRUE`

DNSSUFFIX

Specifies a DNS domain for clients to locate management points that are published in DNS. When a management point is located, it informs the client about other management points in the hierarchy. This behavior means that the management point that is located by using DNS publishing doesn't have to be from the client's site, but can be any management point in the hierarchy.

> **NOTE**
> You don't have to specify this property if the client is in the same domain as a published management point. In that case, the client's domain is automatically used to search DNS for management points.

For more information about DNS publishing as a service location method for Configuration Manager clients, see Service location and how clients determine their assigned management point.

> **NOTE**
> By default, DNS publishing isn't enabled in Configuration Manager.

Example: `CCMSetup.exe SMSSITECODE=ABC DNSSUFFIX=contoso.com`

FSP

Specifies the fallback status point that receives and processes state messages sent by Configuration Manager client computers.

For more information about the fallback status point, see Determine if you need a fallback status point.

Example: `CCMSetup.exe FSP=SMSFP01`

IGNOREAPPVVERSIONCHECK

Specifies that the presence of the minimum required version of Microsoft Application Virtualization (App-V) isn't checked before the client is installed.

> **IMPORTANT**
> If you install the Configuration Manager client without installing App-V, you can't deploy virtual applications.

Example: `CCMSetup.exe IGNOREAPPVVERSIONCHECK=TRUE`

NOTIFYONLY

Specifies that the client reports status, but doesn't remediate problems that it finds.

Example: `CCMSetup.exe NOTIFYONLY=TRUE`

For more information, see How to configure client status.

RESETKEYINFORMATION

If a client has the wrong Configuration Manager trusted root key and can't contact a trusted management point to receive the new trusted root key, use this property to manually remove the old trusted root key. This situation may occur when you move a client from one site hierarchy to another. This property applies to clients that use HTTP and HTTPS client communication.

Example: `CCMSetup.exe RESETKEYINFORMATION=TRUE`

SITEREASSIGN

Enables automatic site reassignment for client upgrades when used with SMSSITECODE=AUTO.

Example: `CCMSetup.exe SMSSITECODE=AUTO SITEREASSIGN=TRUE`

SMSCACHEDIR

Specifies the location of the client cache folder on the client computer, which stores temporary files. By default, the location is *%Windir%\ccmcache*.

Example: `CCMSetup.exe SMSCACHEDIR="C:\Temp"`

This property can be used in conjunction with the SMSCACHEFLAGS property to control the client cache folder location.

Example: `CCMSetup.exe SMSCACHEDIR=Cache SMSCACHEFLAGS=MAXDRIVE` installs the client cache folder on the largest available client disk drive.

SMSCACHEFLAGS

Specifies further installation details for the client cache folder. You can use SMSCACHEFLAGS properties individually or in combination, separated by semicolons. If this property isn't specified, the client cache folder is installed according to the SMSCACHEDIR property, the folder isn't compressed, and the SMSCACHESIZE value is used as the size in MB of the folder.

This setting is ignored when you upgrade an existing client.

Properties:

- PERCENTDISKSPACE: Specifies the folder size as a percentage of the total disk space. If you specify this property, you must also specify the property SMSCACHESIZE as the percentage value to use.
- PERCENTFREEDISKSPACE: Specifies the folder size as a percentage of the free disk space. If you specify

this property, you must also specify the property SMSCACHESIZE as the percentage value to use. For example, if the disk has 10 MB free and SMSCACHESIZE is specified as 50, the folder size is set to 5 MB. You cannot use this property with the PERCENTDISKSPACE property.

- MAXDRIVE: Specifies that the folder should be installed on the largest available disk. This value is ignored if a path has been specified with the SMSCACHEDIR property.
- MAXDRIVESPACE: Specifies that the folder should be installed on the disk drive that has the most free space. This value is ignored if a path has been specified with the SMSCACHEDIR property.
- NTFSONLY: Specifies that the folder can be installed only on NTFS disk drives. This value is ignored if a path has been specified with the SMSCACHEDIR property.
- COMPRESS: Specifies that the folder should be stored in a compressed form.
- FAILIFNOSPACE: Specifies that the client software should be removed if there is insufficient space to install the folder.

Example: `CCMSetup.exe SMSCACHEFLAGS=NTFSONLY;COMPRESS`

SMSCACHESIZE

> **IMPORTANT**
> Client settings are available for specifying the client cache folder size. The addition of those client settings effectively replaces using SMSCACHESIZE as a client.msi property to specify the size of the client cache. For more information, see the client settings for cache size.

> **NOTE**
> If a new package that must be downloaded would cause the folder to exceed the maximum size, and if the folder can't be purged to make sufficient space available, the package download fails, and the program or application doesn't run.

This setting is ignored when you upgrade an existing client, and when the client downloads software updates.

Example: `CCMSetup.exe SMSCACHESIZE=100`

> **NOTE**
> If you reinstall a client, you can't use the SMSCACHESIZE or SMSCACHEFLAGS installation properties to set the cache size to be smaller than it was previously. If you try to do this action, your value is ignored. The cache size is automatically set to the previous size.

SMSCONFIGSOURCE

Specifies the location and order that the Configuration Manager Installer checks for configuration settings. The property is a string of one or more characters, each defining a specific configuration source. Use the character values R, P, M, and U, alone or in combination:

- R: Check for configuration settings in the registry.

  For more information, see information about storing client installation properties in the registry.
- P: Check for configuration settings in the installation properties provided at the command prompt.
- M: Check for existing settings when upgrading an older client with the Configuration Manager client software.

- U: Upgrade the installed client to a newer version (and use the assigned site code).

  By default, the client installation uses `PU` to check first the installation properties and then the existing settings.

  Example: `CCMSetup.exe SMSCONFIGSOURCE=RP`

SMSDIRECTORYLOOKUP

Specifies whether the client can use Windows Internet Name Service (WINS) to find a management point that accepts HTTP connections. Clients use this method when they can't find a management point in Active Directory Domain Services or in DNS.

This property doesn't affect whether the client uses WINS for name resolution.

You can configure two different modes for this property:

- NOWINS: This value is the most secure setting for this property and prevents clients from finding a management point in WINS. When you use this setting, clients must have an alternative method to locate a management point on the intranet, such as Active Directory Domain Services or by using DNS publishing.
- WINSSECURE (default): In this mode, a client that uses HTTP communication can use WINS to find a management point. However, the client must have a copy of the trusted root key before it can successfully connect to the management point. For more information, see Planning for the trusted root key.

Example: `CCMSetup.exe SMSDIRECTORYLOOKUP=NOWINS`

SMSMP

Specifies an initial management point for the Configuration Manager client to use.

> **IMPORTANT**
> If the management point only accepts client connections over HTTPS, you must prefix the management point name with https://.

Example: `CCMSetup.exe SMSMP=smsmp01.contoso.com`

Example: `CCMSetup.exe SMSMP=https://smsmp01.contoso.com`

SMSPUBLICROOTKEY

Specifies the Configuration Manager trusted root key when it cannot be retrieved from Active Directory Domain Services. This property applies to clients that use HTTP and HTTPS client communication. For more information, see Planning for the trusted root key.

Example: `CCMSetup.exe SMSPUBLICROOTKEY=<key\>`

SMSROOTKEYPATH

Used to reinstall the Configuration Manager trusted root key. Specifies the full path and file name to a file containing the trusted root key. This property applies to clients that use HTTP and HTTPS client communication. For more information, see Planning for the trusted root key.

Example: 'CCMSetup.exe SMSROOTKEYPATH=<Full path and filename>`

SMSSIGNCERT

Specifies the full path and .cer file name of the exported self-signed certificate on the site server.

This certificate is stored in the **SMS** certificate store and has the Subject name **Site Server** and the friendly name **Site Server Signing Certificate**.

Example: **CCMSetup.exe /UsePKICert SMSSIGNCERT=<Full path and file name>**

SMSSITECODE

Specifies the Configuration Manager site to assign the client to. This value can either be a three-character site code or the word AUTO. If you specify AUTO, or do not specify this property, the client attempts to determine its site assignment from Active Directory Domain Services or from a specified management point. To enable AUTO for client upgrades, you must also set SITEREASSIGN to TRUE.

> **NOTE**
> Don't use AUTO if you also specify the internet-based management point (CCMHOSTNAME). In that case, you must directly assign the client to its site.

Example: `CCMSetup.exe SMSSITECODE=XZY`

Supported attribute values for the PKI certificate selection criteria

Configuration Manager supports the following attribute values for the PKI certificate selection criteria:

OID ATTRIBUTE	DISTINGUISHED NAME ATTRIBUTE	ATTRIBUTE DEFINITION
0.9.2342.19200300.100.1.25	DC	Domain component
1.2.840.113549.1.9.1	E or E-mail	Email address
2.5.4.3	CN	Common name
2.5.4.4	SN	Subject name
2.5.4.5	SERIALNUMBER	Serial number
2.5.4.6	C	Country code
2.5.4.7	L	Locality
2.5.4.8	S or ST	State or province name
2.5.4.9	STREET	Street address
2.5.4.10	O	Organization name
2.5.4.11	OU	Organizational unit
2.5.4.12	T or Title	Title
2.5.4.42	G or GN or GivenName	Given name
2.5.4.43	I or Initials	Initials
2.5.29.17	(no value)	Subject Alternative Name

About client installation properties published to Active Directory Domain Services

9/11/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

When you extend the Active Directory schema for Configuration Manager, and the site is published to Active Directory Domain Services, many client installation properties are published to Active Directory Domain Services. If a computer can locate these client installation properties, it can use them during Configuration Manager client deployment.

The advantages of using Active Directory Domain Services to publish client installation properties include the following:

- Software update point-based client installations and Group Policy client installations do not require setup parameters to be set up on each computer.
- Because this information is automatically generated, the risk of human error associated with manually entering installation properties is eliminated.

> **NOTE**
> For more information about how to extend the Active Directory schema for Configuration Manager, and how to publish a site, see Schema extensions for System Center Configuration Manager.

Client installation properties published to Active Directory Domain Services

The following is a list of client installation properties. For more information about each item listed below, see About client installation properties in System Center Configuration Manager.

- The Configuration Manager site code.
- The site server signing certificate.
- The trusted root key.
- The client communication ports for HTTP and HTTPS.
- The fallback status point. If the site has multiple fallback status points, only the first one that was installed is published to Active Directory Domain Services.
- A setting to indicate that the client must communicate by using HTTPS only.
- Settings related to PKI certificates:
  - Whether to use a client PKI certificate.
  - The selection criteria for certificate selection. This may be required because the client has more than one valid PKI certificate that can be used for Configuration Manager.
  - A setting to determine which certificate to use if the client has multiple valid certificates after the certificate selection process.

    - The certificate issuers list that contains a list of trusted root CA certificates.

- Client.msi installation properties that are specified in the **Client** tab of the **Client Push Installation Properties** dialog box.

Client installation (CCMSetup) uses the properties that are published to Active Directory Domain Services only if no other properties are specified by using either of the following:

- The manual installation method (described later in this article)
- The Group Policy installation method (described later in this article)

> **NOTE**
> The client installation properties are used to install the client. These properties might be overwritten with new settings from its assigned site after the client is installed and has successfully been assigned to a Configuration Manager site.

Use the details in the following sections to determine which Configuration Manager client installation methods use Active Directory Domain Services to obtain client installation properties.

Client push installation

Client push installation does not use Active Directory Domain Services to obtain installation properties.

Instead, you can specify client installation properties in the **Installation Properties** tab of the **Client Push Installation Properties** dialog box. These options and client-related site settings are stored in a file that the client reads during client installation.

> **NOTE**
> You do not have to specify any CCMSetup properties for client push installation, or the fallback status point, or the trusted root key in the **Installation Properties** tab. These settings are automatically supplied to clients when they are installed by using client push installation. In addition to Client.msi properties, CCMSetup supports the following parameters: /forcereboot, /skipprereq, /logon, /BITSPriority, /downloadtimeout, /forceinstall

Any properties that you specify in the **Installation Properties** tab are published to Active Directory Domain Services if the site is published to Active Directory Domain Services. These settings are read by client installations where CCMSetup is run with no installation properties.

Software update point-based installation

The software update point-based installation method does not support the addition of installation properties to the CCMSetup command line.

If no command line properties have been provisioned on the client computer by using Group Policy, CCMSetup searches Active Directory Domain Services for installation properties.

Group Policy installation

The Group Policy installation method does not support the addition of installation properties to the CCMSetup command line.

If no command line properties have been provisioned on the client computer, CCMSetup searches Active Directory Domain Services for installation properties.

Manual installation

CCMSetup searches Active Directory Domain Services for installation properties under the following circumstances:

- No command line properties are specified after the CCMSetup.exe command.
- The computer has not been provisioned with installation properties by using Group Policy.

Logon script installation

CCMSetup searches Active Directory Domain Services for installation properties under the following circumstances:

- No command line properties are specified after the CCMSetup.exe command.
- The computer has not been provisioned with installation properties by using Group Policy.

Software distribution installation

CCMSetup searches Active Directory Domain Services for installation properties under the following circumstances:

- No command line properties are specified after the CCMSetup.exe command.
- The computer has not been provisioned with installation properties by using Group Policy.

Installations for clients that cannot access Active Directory Domain Services

These client computers cannot read or access the published installation properties from Active Directory Domain Services.

These clients include:

- Workgroup computers.
- Clients that are assigned to a Configuration Manager site that is not published to Active Directory Domain Services.
- Clients that are installed when they are on the Internet.

How to deploy clients to UNIX and Linux servers in Configuration Manager

9/5/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

> **IMPORTANT**
>
> Starting in version 1902, Configuration Manager doesn't support Linux or UNIX clients.
>
> Consider Microsoft Azure Management for managing Linux servers. Azure solutions have extensive Linux support that in most cases exceed Configuration Manager functionality, including end-to-end patch management for Linux.

Before you can manage a Linux or UNIX server with Configuration Manager, you must install the Configuration Manager client for Linux and UNIX on each Linux or UNIX server. You can accomplish the installation of the client manually on each computer, or use a shell script that installs the client remotely. Configuration Manager doesn't support the use of client push installation for Linux or UNIX servers. Optionally you can configure a Runbook for System Center Orchestrator to automate the install of the client on the Linux or UNIX server.

Regardless of the installation method you use, the install process requires the use of a script named **install** to manage the install process. This script is included when you download the Client for Linux and UNIX.

The install script for the Configuration Manager client for Linux and UNIX supports command-line properties. Some command-line properties are required, while others are optional. For example, when you install the client, you must specify a management point from the site that is used by the Linux or UNIX server for its initial contact with the site. For the complete list of command-line properties, see Command-line properties for installing the client on Linux and UNIX servers.

After you install the client, you specify Client Settings in the Configuration Manager console to configure the client agent in the same way you would Windows-based clients. For more information, see Client settings for Linux and UNIX servers.

About client installation packages and the universal agent

To install the client for Linux and UNIX on a specific platform, you must use the applicable client installation package for the computer where you install the client. Applicable client installation packages are included as part of each client download from the Microsoft Download Center. In addition to client installation packages, the client download includes the **install** script that manages the installation of the client on each computer.

When you install a client, you can use the same process and command-line properties regardless of the client installation package you use.

For information about the operating systems, platforms, and client installation packages that are supported by each release of the Configuration Manager client for Linux and UNIX, see Linux and UNIX servers.

Install the client on Linux and UNIX servers

To install the client for Linux and UNIX, you run a script on each Linux or UNIX computer. The script is named **install** and supports command-line properties that modify the installation behavior and reference the client installation package. The install script and client installation package must be located on the client. The client installation package contains the Configuration Manager client files for a specific Linux or UNIX operating system

and platform. Each client installation package contains all the necessary files to complete the client installation and unlike Windows-based computers, doesn't download additional files from a management point or other source location.

After you install the Configuration Manager client for Linux and UNIX, you don't need to reboot the computer. As soon as the software installation is complete, the client is operational. If you reboot the computer, the Configuration Manager client restarts automatically.

The installed client runs with root credentials. Root credentials are required to collect hardware inventory and do software deployments.

Use the following command format:

```
./install -mp <computer> -sitecode <sitecode> <property #1> <property #2> <client installation package>
```

- `install` is the name of the script file that installs the client for Linux and UNIX. This file is provided with the client software.
- `-mp <computer>` specifies the initial management point that is used by the client. Example: `smsmp.contoso.com`
- `-sitecode <site code>` specifies the site code that the client is assigned to. Example: `S01`
- `<property #1> <property #2>` specifies the command-line properties to use with the installation script.

  > **NOTE**
  > For more information, see Command-line properties for installing the client on Linux and UNIX servers.

- **client installation package** is the name of the client installation .tar package for this computer operating system, version, and CPU architecture. The client installation .tar file must be specified last. Example: `ccm-Universal-x64.<build>.tar`

To install the Configuration Manager client on Linux and UNIX servers

1. On a Windows computer, download the appropriate client file for the Linux or UNIX server you want to manage.
2. Run the self-extracting .exe file on the Windows computer to extract the install script and the client installation .tar file.
3. Copy the **install** script and the .tar file to a folder on the server you want to manage.
4. On the UNIX or Linux server, run the following command to enable the script to run as a program: `chmod +x install`

   > **IMPORTANT**
   > You must use root credentials to install the client.

5. Next, run the following command to install the Configuration Manager client: `./install -mp <hostname> -sitecode <code> ccm-Universal-x64.<build>.tar`

   When you enter this command, use additional command-line properties you require. For the list of command-line properties, see Command-line properties for installing the client on Linux and UNIX servers
6. After the script runs, validate the install by reviewing the **/var/opt/microsoft/scxcm.log** file. Additionally, you can confirm that the client is installed and communicating with the site by viewing details for the client

in the **Devices** node of the **Assets and Compliance** workspace in the Configuration Manager console.

Command-line properties for installing the client on Linux and UNIX servers

The following properties are available to modify the behavior of the install script:

> **NOTE**
> Use the property `-h` to display this list of supported properties.

- `-mp <server FQDN>`

  Required. Specifies by FQDN, the management point server that the client uses as an initial point of contact.

  > **IMPORTANT**
  > This property doesn't specify the management point to which the client is assigned after installation.

  > **NOTE**
  > When you use the `-mp` property to specify a management point that's configured to accept only HTTPS client connections, you must also use the `-UsePKICert` property.

- `-sitecode <sitecode>`

  Required. Specifies the Configuration Manager primary site to assign the Configuration Manager client to. Example: `-sitecode S01`

- `-fsp <server_FQDN>`

  Optional. Specifies by FQDN, the fallback status point server that the client uses to submit state messages. For more information, see Determine whether you require a fallback status point.

- `-dir <directory>`

  Optional. Specifies an alternate location to install the Configuration Manager client files. By default, the client installs to the following location: `/opt/microsoft`

- `-nostart`

  Optional. Prevents the automatic start of the Configuration Manager client service, **ccmexec.bin**, after the client installation completes.

  After the client installs, you must start the client service manually.

  By default, the client service starts after the client installation completes, and each time the computer restarts.

- `-clean`

  Optional. Specifies the removal of all client files and data from a previously installed client for Linux and UNIX, before the new installation starts. This action removes the client's database and certificate store.

- `-keepdb`

  Optional. Specifies that the local client database is kept, and reused when you reinstall a client. By default, when you reinstall a client this database is deleted.

- `-UsePKICert <parameter>`

  Optional. Specifies the full path and file name to a X.509 PKI certificate in the Public Key Certificate Standard (PKCS#12) format. This certificate is used for client authentication. If a certificate is not specified during installation and you need to add or change a certificate, use the **certutil** utility. For more information, see How to manage certificates on the client for Linux and UNIX.

  When you use `-UsePKICert`, you must also supply the password associated with the PKCS#12 file by use of the `-certpw` command-line parameter.

  If you don't use this property to specify a PKI certificate, the client uses a self-signed certificate and all communications to site systems are over HTTP.

  If you specify an invalid certificate on the client install command line, no errors are returned. Certificate validation occurs after the client installs. When the client starts, certificates are validated with the management point. If a certificate fails validation, the following message appears in **scxcm.log**: **Failed validate the certificate for Management Point**. The default log file location is: **/var/opt/microsoft/scxcm.log**.

  > **NOTE**
  > You must specify this property when you install a client and use the `-mp` property to specify a management point that is configured to accept only HTTPS client connections.

  Example: `-UsePKICert <full path and filename> -certpw <password>`

- `-certpw <parameter>`

  Optional. Specifies the password associated with the PKCS#12 file that you specified by use of the `-UsePKICert` property.

  Example: `-UsePKICert <full path and filename> -certpw <password>`

- `-NoCRLCheck`

  Optional. Specifies that a client shouldn't check the certificate revocation list (CRL) when it communicates over HTTPS by use of a PKI certificate. When this option isn't specified, the client checks the CRL before establishing an HTTPS connection by use of PKI certificates. For more information about client CRL checking, see Planning for PKI Certificate Revocation.

  Example: `-UsePKICert <full path and filename> -certpw <password> -NoCRLCheck`

- `-rootkeypath <file location>`

  Optional. Specifies the full path and file name to the Configuration Manager trusted root key. The Configuration Manager trusted root key provides a mechanism that Linux and UNIX clients use to verify that they're connected to a site system that belongs to the correct hierarchy.

  If you don't specify the trusted root key on the command line, the client will trust the first management point it communicates with and will automatically retrieve the trusted root key from that management point.

  For more information, see Planning for the Trusted Root Key.

  Example: `-rootkeypath <full path and filename>`

- `-httpport <port>`

  Optional. Specifies the port that is configured on management points that the client uses when communicating to management points over HTTP. If the port isn't specified, the default value of 80 is used.

Example: `-httpport 80`

- `-httpsport <port>`

  Optional. Specifies the port that is configured on management points that the client uses when communicating to management points over HTTPS. If the port isn't specified, the default value of 443 is used.

  Example: `-UsePKICert <full path and certificate name> -httpsport 443`

- `-ignoreSHA256validation`

  Optional. Specifies that client installation skips SHA-256 validation. Use this option when installing the client on operating systems that didn't release with a version of OpenSSL that supports SHA-256. For more information, see About Linux and UNIX operating systems that don't support SHA-256.

- `-signcertpath <file location>`

  Optional. Specifies the full path and **.cer** file name of the exported self-signed certificate on the site server. If PKI certificates aren't available, the Configuration Manager site server automatically generates self-signed certificates.

  These certificates are used to validate that the client policies downloaded from the management point were sent from the intended site. If a self-signed certificate is not specified during installation, or you need to change the certificate, use the **certutil** utility. For more information, see How to manage certificates on the client for Linux and UNIX.

  This certificate can be retrieved through the **SMS** certificate store and has the Subject name **Site Server** and the friendly name **Site Server Signing Certificate**.

  If this option isn't specified during installation, Linux and UNIX clients trust the first management point they communicate with. They automatically retrieve the signing certificate from that management point.

  Example: `-signcertpath <full path and file name>`

- `-rootcerts`

  Optional. Specifies additional PKI certificates to import that aren't part of a management points certification authority (CA) hierarchy. If you specify multiple certificates in the command line, they should be comma delimited.

  Use this option if you use PKI client certificates that don't chain to a root CA certificate that is trusted by your sites management points. Management points will reject the client if the client certificate doesn't chain to a trusted root certificate in the site's certificate issuers list.

  If you don't use this option, the Linux and UNIX client will verify the trust hierarchy using only the certificate in the `-UsePKICert` option.

  Example: `-rootcerts <full path and file name>,<full path and file name>`

Uninstalling the client from Linux and UNIX servers

To uninstall the Configuration Manager client for Linux and UNIX you use the uninstall utility, **uninstall**. By default, this file is located in the **/opt/microsoft/configmgr/bin/** folder on the client computer. This uninstall command doesn't support any command-line parameters and will remove all files related to the client software from the server.

To uninstall the client, use the following command line: **/opt/microsoft/configmgr/bin/uninstall**

You don't have to reboot the computer after you uninstall the Configuration Manager client for Linux and UNIX.

Configure Request Ports for the Client for Linux and UNIX

Similar to Windows-based clients, the Configuration Manager client for Linux and UNIX uses HTTP and HTTPS to communicate with Configuration Manager site systems. The ports that the Configuration Manager client uses to communicate are referred to as a request ports.

When you install the Configuration Manager client for Linux and UNIX, you can change the clients default request ports by specifying the **-httpport** and **-httpsport** installation properties. When you don't specify the installation property and a custom value, the client uses the default values. The default values are **80** for HTTP traffic and **443** for HTTPS traffic.

After you install the client, you can't change its request port configuration. Instead, to change the port configuration you must reinstall the client and specify the new port configuration. When you reinstall the client to change the request port numbers, run the **install** command similar to the new client install, but use the additional command-line property of **-keepdb**. This switch instructs the installation to keep the client database and files including the clients GUID and certificate store.

For more information about client communication port numbers, see How to configure client communication ports in System Center Configuration Manager.

Configure the Client for Linux and UNIX to Locate Management Points

When you install the Configuration Manager client for Linux and UNIX, you must specify a management point to use as an initial point of contact.

The Configuration Manager client for Linux and UNIX contacts this management point at the time the client installs. If the client fails to contact the management point, the client software continues to retry until successful.

For more information about how clients locate management points, see Locating Management Points.

Linux and UNIX clients component services and commands for Configuration Manager

3/27/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

IMPORTANT

Starting in version 1902, Configuration Manager doesn't support Linux or UNIX clients.

Consider Microsoft Azure Management for managing Linux servers. Azure solutions have extensive Linux support that in most cases exceed Configuration Manager functionality, including end-to-end patch management for Linux.

The following table identifies the client component services of the Configuration Manager client for Linux and UNIX.

FILE NAME	MORE INFORMATION
ccmexec.bin	This service is similar to the ccmexc service on a Windows-based client. It's responsible for all communications with Configuration Manager site system roles, and also communicates with the omiserver.bin service to collect hardware inventory from the local computer. For a list of supported command-line arguments, run `ccmexec -h`
omiserver.bin	This service is the CIM server. The CIM server provides a framework for pluggable software modules called providers. Providers interact with Linux and UNIX computer resources and collect the hardware inventory data. For example, the **process provider** for a Linux computer collects data associated with the Linux operating system processes.

The following tables list commands that you can use to start, stop, or restart the client services (ccmexec.bin and omiserver.bin) on each version of Linux or UNIX. When you start or stop the ccmexec service, the omiserver service also starts or stops.

OPERATING SYSTEM	COMMANDS
Universal Agent RHEL 4 and SLES 9	Start: `/etc/init d/ccmexecd start` Stop: `/etc/init d/ccmexecd stop` Restart: `/etc/init d/ccmexecd restart`
Solaris 9	Start: `/etc/init d/ccmexecd start` Stop: `/etc/init d/ccmexecd stop` Restart: `/etc/init d/ccmexecd restart`

OPERATING SYSTEM	COMMANDS

Solaris 10	Start:
	`svcadm enable -s svc:/application/management/omiserver`
	`svcadm enable -s svc:/application/management/ccmexecd`
	Stop:
	`svcadm disable -s svc:/application/management/ccmexecd`
	`svcadm disable -s svc:/application/management/omiserver`

Solaris 11	Start:
	`svcadm enable -s svc:/application/management/omiserver`
	`svcadm enable -s svc:/application/management/ccmexecd`
	Stop:
	`svcadm disable -s svc:/application/management/ccmexecd`
	`svcadm disable -s svc:/application/management/omiserver`

AIX	Start:
	`startsrc -s omiserver`
	`startsrc -s ccmexec`
	Stop:
	`stopsrc -s ccmexec`
	`stopsrc -s omiserver`

HP-UX	Start: `/sbin/init.d/ccmexecd start` Stop: `/sbin/init.d/ccmexecd stop` Restart: `/sbin/init.d/ccmexecd restart`

Prepare to deploy client software to Macs

9/5/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Follow these steps to make sure that you're ready to deploy the Configuration Manager client to Mac computers.

Mac prerequisites

The Mac client installation package isn't supplied with the Configuration Manager media. Download the **Clients for additional operating systems** from the Microsoft Download Center.

For the list of supported versions, see Supported operating systems for clients and devices.

Certificate requirements

Client installation and management for Mac computers requires public key infrastructure (PKI) certificates. PKI certificates secure the communication between the Mac computers and the Configuration Manager site by using mutual authentication and encrypted data transfers. Configuration Manager can request and install a user client certificate. It uses Certificate Services with an enterprise certification authority, and the Configuration Manager enrollment point and enrollment proxy point. You can also request and install a computer certificate independently from Configuration Manager. This certificate must meet the Configuration Manager certificate requirements.

Configuration Manager Mac clients always check for certificate revocation. You can't disable this function.

If Mac clients can't locate the certificate revocation list (CRL), they can't connect to Configuration Manager site systems. Especially for Mac clients in a different forest to the issuing certification authority, check your CRL design. Make sure that Mac clients can locate and download a CRL.

Before you install the Configuration Manager client on a Mac computer, decide how to install the client certificate:

- Use Configuration Manager enrollment by using the CMEnroll tool. The enrollment process doesn't support automatic certificate renewal. Re-enroll Mac computers before the certificate expires.
- Use a certificate request and installation method that's independent from Configuration Manager.

For more information about Mac client certificate requirements, see PKI certificate requirements for Configuration Manager.

Mac clients are automatically assigned to the Configuration Manager site that manages them. Mac clients install as internet-only clients, even if communication is restricted to the intranet. This configuration means that they communicate with internet-enabled management points and distribution points in their assigned site. Mac computers don't communicate with site systems outside their assigned site.

> **IMPORTANT**
> The Configuration Manager client for macOS can't be used to connect to a management point that's configured to use a database replica.

Deploy a web server certificate to site system servers

If these site systems don't have it, deploy a web server certificate to the computers that have these site system

roles:

- Management point
- Distribution point
- Enrollment point
- Enrollment proxy point

The web server certificate must include the internet FQDN that's specified in the site system properties. The server doesn't have to be accessible from the internet to support Mac computers. If you don't require internet-based client management, you can specify the intranet FQDN value for the internet FQDN.

Specify the site system's internet FQDN value in the web server certificate for the management point, the distribution point, and the enrollment proxy point.

For more information of an example deployment, see Deploying the web server certificate for site systems that run IIS.

Deploy a client authentication certificate to site system servers

If these site systems don't have it, deploy a client authentication certificate to the computers that host these site system roles:

- Management point
- Distribution point

For an example deployment that creates and installs the client certificate for management points, see the Deploying the client certificate for Windows computers.

For an example deployment that creates and installs the client certificate for distribution points, see the Deploying the client certificate for distribution points.

> **IMPORTANT**
> To deploy the client to devices running macOS Sierra, the subject name of the management point certificate must be configured correctly. For example, use the FQDN of the management point server.

Prepare the client certificate template for Macs

The certificate template must have **Read** and **Enroll** permissions for the user account that enrolls the certificate on the Mac computer.

For more information, see Deploying the client certificate for Mac computers.

Configure the management point and distribution point

Configure management points for the following options:

- HTTPS
- Allow client connections from the internet. This configuration value is required to manage Mac computers. However, it doesn't mean that site system servers must be accessible from the internet.
- Allow mobile devices and Mac computers to use this management point

Distribution points aren't required to install the client for Mac. If you want to deploy software to these computers

after you install the client, configure distribution points to allow client connections from the internet.

To configure management points and distribution points to support Macs

Before you start this procedure, make sure to configure the management point and distribution point with an internet FQDN. If these servers don't support internet-based client management, specify the intranet FQDN as the internet FQDN value.

The site system roles must be in a primary site.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Servers and Site System Roles** node. Then select the server that has the right site system roles.
2. In the details pane, select the **Management point** role, and select **Properties** in the ribbon. In the **Management point Properties** window, configure these options:
   a. Choose **HTTPS**.
   b. Choose **Allow internet-only client connections** or **Allow intranet and internet client connections**. These options require an internet or intranet FQDN.
   c. Choose **Allow mobile devices and Mac computers to use this management point**.
   d. Select **OK** to save this configuration.
3. In the details pane of the Server and Site System Roles node, select the **Distribution point** role, and select **Properties** in the ribbon. In the **Distribution point Properties** window, configure these options:
   - Choose **HTTPS**.
   - Choose **Allow internet-only client connections** or **Allow intranet and internet client connections**. These options require an internet or intranet FQDN.
   - Choose **Import certificate**, browse to the exported client distribution point certificate file, and then specify the password.
4. Repeat this procedure for all management points and distribution points in primary sites that manage Mac computers.

Configure the enrollment proxy point and the enrollment point

Install both roles in the same site. You don't have to install them on the same site system server, or in the same Active Directory forest.

For more information about site system role placement and considerations, see Site system roles.

These procedures configure the site system roles to support Mac computers:

- New site system server
- Existing site system server

In either case, on the **System Role Selection** page, select **Enrollment proxy point** and **Enrollment point** from the list of available roles.

Install the reporting services point

For more information, see Install the reporting services point.

Next steps

How to deploy clients to Macs

9/11/2019 • 9 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article describes how to deploy and maintain the Configuration Manager client on Mac computers. To learn about what you have to configure before deploying clients to Mac computers, see Prepare to deploy client software to Macs.

When you install a new client for Mac computers, you might have to also install Configuration Manager updates to reflect the new client information in the Configuration Manager console.

In these procedures, you have two options for installing client certificates. Read more about client certificates for Macs in Prepare to deploy client software to Macs.

- Use Configuration Manager enrollment by using the CMEnroll tool. The enrollment process doesn't support automatic certificate renewal. Re-enroll the Mac computer before the installed certificate expires.
- Use a certificate request and installation method that is independent from Configuration Manager.

> **IMPORTANT**
> To deploy the client to devices running macOS Sierra, correctly configure the **Subject name** of the management point certificate. For example, use the FQDN of the management point server.

Configure client settings

Use the default client settings to configure enrollment for Mac computers. You can't use custom client settings. To request and install the certificate, the Configuration Manager client for Mac requires the default client settings.

1. In the Configuration Manager console, go to the **Administration** workspace. Select the **Client Settings** node, and then select **Default Client Settings**.
2. On the **Home** tab of the ribbon, in the **Properties** group, choose **Properties**.
3. Select the **Enrollment** section, and then configure the following settings:
   a. **Allow users to enroll mobile devices and Mac computers**: **Yes**
   b. **Enrollment profile:** Choose **Set Profile**.
4. In the **Mobile Device Enrollment Profile** dialog box, choose **Create**.
5. In the **Create Enrollment Profile** dialog box, enter a name for this enrollment profile. Then configure the **Management site code**. Select the Configuration Manager primary site that contains the management points for these Mac computers.

   > **NOTE**
   > If you can't select the site, make sure that you configure at least one management point in the site to support mobile devices.

6. Choose **Add**.

7. In the **Add Certification Authority for Mobile Devices** window, select the certification authority server that issues certificates to Mac computers.
8. In the **Create Enrollment Profile** dialog box, select the Mac computer certificate template that you previously created.
9. Select **OK** to close the **Enrollment Profile** dialog box, and then the **Default Client Settings** dialog box.

> **TIP**
> If you want to change the client policy interval, use **Client policy polling interval** in the **Client Policy** client setting group.

The next time the devices download client policy, Configuration Manager applies these settings for all users. To initiate policy retrieval for a single client, see Initiate policy retrieval for a Configuration Manager client.

In addition to the enrollment client settings, make sure that you have configured the following client device settings:

- **Hardware inventory**: Enable and configure this feature if you want to collect hardware inventory from Mac and Windows client computers. For more information, see How to extend hardware inventory.
- **Compliance settings**: Enable and configure this feature if you want to evaluate and remediate settings on Mac and Windows client computers. For more information, see Plan for and configure compliance settings.

For more information, see How to configure client settings.

Download the Mac client

1. Download the Mac OS X client file package from the Microsoft Download Center. Save **ConfigmgrMacClient.msi** to a computer that runs Windows. This file isn't on the Configuration Manager installation media.
2. Run the installer on the Windows computer. Extract the Mac client package, **Macclient.dmg**, to a folder on the local disk. The default path is `C:\Program Files (x86)\Microsoft\System Center 2012 Configuration Manager Mac Client`.
3. Copy the **Macclient.dmg** file to a folder on the Mac computer.
4. On the Mac computer, run **Macclient.dmg** to extract the files to a folder on the local disk.
5. In the folder, make sure that it contains the following files:
   - **Ccmsetup**: Installs the Configuration Manager client on your Mac computers using **CMClient.pkg**
   - **CMDiagnostics**: Collects diagnostic information related to the Configuration Manager client on your Mac computers
   - **CMUninstall**: Uninstalls the client from your Mac computers
   - **CMAppUtil**: Converts Apple application packages into a format that you can deploy as a Configuration Manager application
   - **CMEnroll**: Requests and installs the client certificate for a Mac computer so that you can then install the Configuration Manager client

Enroll the Mac client

Enroll individual clients with the Mac computer enrollment wizard.

To automate enrollment for many clients, use the CMEnroll tool.

Enroll the client with the Mac computer enrollment wizard

1. After you install the client, the Computer Enrollment wizard opens. To manually start the wizard, select **Enroll** from the **Configuration Manager** preference page.

2. On the second page of the wizard, provide the following information:

   - **User name**: The user name can be in the following formats:

     - `domain\name`. For example: `contoso\mnorth`
     - `user@domain`. For example: `mnorth@contoso.com`

     > **IMPORTANT**
     > When you use an email address to populate the **User name** field, Configuration Manager automatically populates the **Server name** field. It uses the default name of the enrollment proxy point server and the domain name of the email address. If these names don't match the name of the enrollment proxy point server, fix the **Server name** during enrollment.

     The user name and corresponding password must match an Active Directory user account that has **Read** and **Enroll** permissions on the Mac client certificate template.

   - **Server name**: The name of the enrollment proxy point server.

Client and certificate automation with CMEnroll

Use this procedure for automation of client installation and requesting and enrollment of client certificates with the CMEnroll tool. To run the tool, you must have an Active Directory user account.

1. On the Mac computer, navigate to the folder where you extracted the contents of the **Macclient.dmg** file.

2. Enter the following command: `sudo ./ccmsetup`

3. Wait until you see the **Completed installation** message. Although the installer displays a message that you must restart now, don't restart, and continue to the next step.

4. From the **Tools** folder on the Mac computer, type the following command:
   `sudo ./CMEnroll -s <enrollment_proxy_server_name> -ignorecertchainvalidation -u '<user_name>'`

   After the client installs, the Mac Computer Enrollment wizard opens to help you enroll the Mac computer. For more information, see Enroll the client by using the Mac computer enrollment wizard.

   Example: If the enrollment proxy point server is named **server02.contoso.com**, and you grant **contoso\mnorth** permissions for the Mac client certificate template, type the following command:
   `sudo ./CMEnroll -s server02.contoso.com -ignorecertchainvalidation -u 'contoso\mnorth'`

   > **NOTE**
   > If the user name includes any of the following characters, enrollment fails: `<>"+=,`. Use an out-of-band certificate with a user name that doesn't include these characters.
   >
   > For a more seamless user experience, script the installation steps. Then users only have to supply their user name and password.

5. Type the password for the Active Directory user account. When you enter this command, it prompts for two passwords. The first password is for the super user account to run the command. The second prompt is for the Active Directory user account. The prompts look identical, so make sure that you specify them in the

correct sequence.

6. Wait until you see the **Successfully enrolled** message.
7. To limit the enrolled certificate to Configuration Manager, on the Mac computer, open a terminal window and make the following changes:
   a. Enter the command `sudo /Applications/Utilities/Keychain Access.app/Contents/MacOS/Keychain Access`
   b. In the **Keychain Access** window, in the **Keychains** section, choose **System**. Then in the **Category** section, choose **Keys**.
   c. Expand the keys to view the client certificates. Find the certificate with a private key that you installed, and open the key.
   d. On the **Access Control** tab, choose **Confirm before allowing access**.
   e. Browse to **/Library/Application Support/Microsoft/CCM**, select **CCMClient**, and then choose **Add**.
   f. Choose **Save Changes** and close the **Keychain Access** dialog box.
8. Restart the Mac computer.

To verify that the client installation is successful, open the **Configuration Manager** item in **System Preferences** on the Mac computer. Also update and view the **All Systems** collection in the Configuration Manager console. Confirm that the Mac computer appears in this collection as a managed client.

> **TIP**
> To help troubleshoot the Mac client, use the **CMDiagnostics** tool included with the Mac client package. Use it to collect the following diagnostic information:
>
> - A list of running processes
> - The Mac OS X operating system version
> - Mac OS X crash reports relating to the Configuration Manager client including **CCM*.crash** and **System Preference.crash**.
> - The Bill of Materials (BOM) file and property list (.plist) file created by the Configuration Manager client installation.
> - The contents of the folder **/Library/Application Support/Microsoft/CCM/Logs**.
>
> The information collected by CmDiagnostics is added to a zip file that is saved to the desktop of the computer and is named `cmdiag-<hostname>-<datetime>.zip`

Manage certificates external to Configuration Manager

You can use a certificate request and installation method independent from Configuration Manager. Use the same general process, but include the following additional steps:

- When you install the Configuration Manager client, use the **MP** and **SubjectName** command-line options. Enter the following command: `sudo ./ccmsetup -MP <management point internet FQDN> -SubjectName <certificate subject name>`. The certificate subject name is case-sensitive, so type it exactly as it appears in the certificate details.

  Example: The management point's internet FQDN is **server03.contoso.com**. The Mac client certificate has the FQDN of **mac12.contoso.com** as a common name in the certificate subject. Use the following command: `sudo ./ccmsetup -MP server03.contoso.com -SubjectName mac12.contoso.com`

- If you have more than one certificate that contains the same subject value, specify the certificate serial

number to use for the Configuration Manager client. Use the following command: `sudo defaults write com.microsoft.ccmclient SerialNumber -data "<serial number>"`.

For example: `sudo defaults write com.microsoft.ccmclient SerialNumber -data "17D4391A00000003DB"`

Renew the Mac client certificate

This procedure removes the SMSID. The Configuration Manager client for Mac requires a new ID to use a new or renewed certificate.

> **IMPORTANT**
> After you replace the client SMSID, when you delete the old resource in the Configuration Manager console, you also delete any stored client history. For example, hardware inventory history for that client.

1. Create and populate a device collection for the Mac computers that must renew the computer certificates.
2. In the **Assets and Compliance** workspace, start the **Create Configuration Item Wizard**.
3. On the **General** page of the wizard, specify the following information:
   - **Name**: **Remove SMSID for Mac**
   - **Type**: **Mac OS X**
4. On the **Supported Platforms** page, select all Mac OS X versions.
5. On the **Settings** page, select **New**. In the **Create Setting** window, specify the following information:
   - **Name**: **Remove SMSID for Mac**
   - **Setting type**: **Script**
   - **Data type**: **String**
6. In the **Create Setting** window, for **Discovery script**, select **Add script**. This action specifies a script to discover Mac computers configured with an SMSID.
7. In the **Edit Discovery Script** window, enter the following shell script:

   ```
   defaults read com.microsoft.ccmclient SMSID
   ```

8. Choose **OK** to close the **Edit Discovery Script** window.
9. In the **Create Setting** window, for **Remediation script (optional)**, choose **Add script**. This action specifies a script to remove the SMSID when it's found on Mac computers.
10. In the **Create Remediation Script** window, enter the following shell script:

    ```
    defaults delete com.microsoft.ccmclient SMSID
    ```

11. Choose **OK** to close the **Create Remediation Script** window.
12. On the **Compliance Rules** page, choose **New**. Then in the **Create Rule** window, specify the following information:
    - **Name**: **Remove SMSID for Mac**
    - **Selected setting**: Choose **Browse** and then select the discovery script that you previously specified.

- In **the following values** field: **The domain/default pair of (com.microsoft.ccmclient, SMSID) does not exist**.
- Enable the option to **Run the specified remediation script when this setting is noncompliant**.

13. Complete the wizard.
14. Create a configuration baseline that contains this configuration item. Deploy the baseline to the target collection.

    For more information, see How to create configuration baselines.

15. After you install a new certificate on Mac computers that have the SMSID removed, run the following command to configure the client to use the new certificate:

```
sudo defaults write com.microsoft.ccmclient SubjectName -string <subject_name_of_new_certificate>
```

See also

Prepare to deploy clients to Macs

Maintain Mac clients

How to assign clients to a site in System Center Configuration Manager

2/12/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

After a System Center Configuration Manager client is installed, it must join a Configuration Manager primary site before you can manage it. The site that a client joins is called its *assigned site*. Clients cannot be assigned to a central administration site or to a secondary site.

The assignment process happens after the client is successfully installed and determines which site manages the client computer. You can either directly assign the client to a site, or you can use automatic site assignment where the client automatically finds an appropriate site based on its current network location or a fallback site that has been configured for the hierarchy.

When you install the mobile device client during Configuration Manager enrollment, the device is always automatically assigned to a site. When you install the client on a computer, you can choose whether or not to assign the client to a site. However, when the client is installed but not assigned, the client is unmanaged until site assignment is successful.

> **NOTE**
> Always assign clients to sites running the same version of Configuration Manager. Avoid assigning a Configuration Manager client from a newer release to a site from an older release. If necessary, update the primary site to same Configuration Manager version that you are using for the clients.

After the client is assigned to a site, it remains assigned to that site, even if the client changes its IP address and roams to another site. Only an administrator can manually assign the client to another site or remove the client assignment.

> **WARNING**
> An exception to a client remaining assigned to a site is if you assign the client on a Windows Embedded device when the write filters are enabled. If you do not first disable write filters before you assign the client, the site assignment status of the client reverts to its original state when the device next restarts.
>
> For example, if the client is configured for automatic site assignment, it will reassign on startup and might be assigned to a different site. If the client is not configured for automatic site assignment but requires manual site assignment, you must manually reassign the client after startup before you can manage this client again by using Configuration Manager.
>
> To avoid this behavior, disable the write filters before you assign the client on embedded devices, and then enable the write filters after you have verified that site assignment was successful.

If client assignment fails, the client software remains installed, but will be unmanaged. A client is considered unmanaged when it is installed but not assigned to a site, or is assigned to a site but cannot communicate with a management point.

Using Manual Site Assignment for Computers

You can manually assign client computers to a site by using the following two methods:

- Use a client installation property that specifies the site code.
- In Control Panel, in **Configuration Manager**, specify the site code.

> **NOTE**
> If you manually assign a client computer to a Configuration Manager site code that does not exist, the site assignment fails.

Using Automatic Site Assignment for Computers

Automatic site assignment can occur during client deployment, or when you click **Find Site** in the **Advanced** tab of the **Configuration Manager Properties** in the Control Panel. The Configuration Manager client compares its own network location with the boundaries that are configured in the Configuration Manager hierarchy. When the network location of the client falls within a boundary group that is enabled for site assignment, or the hierarchy is configured for a fallback site, the client is automatically assigned to that site without your having to specify a site code.

You can configure boundaries by using one or more of the following:

- IP subnet
- Active Directory site
- IP v6 prefix
- IP address range

> **NOTE**
> If a Configuration Manager client has multiple network adapters and therefore has multiple IP addresses, the IP address used to evaluate client site assignment is assigned randomly.

For information about how to configure boundary groups for site assignment and how to configure a fallback site for automatic site assignment, see Define site boundaries and boundary groups for System Center Configuration Manager.

Configuration Manager clients that use automatic site assignment attempt to find site boundary groups that are published to Active Directory Domain Services. If this fails (for example, the Active Directory schema is not extended for Configuration Manager, or clients are workgroup computers), clients can get boundary group information from a management point.

You can specify a management point for client computers to use when they are installed, or clients can locate a management point by using DNS publishing or WINS.

If the client cannot find a site that is associated with a boundary group that contains its network location, and the hierarchy does not have a fallback site, the client retries every 10 minutes until it can be assigned to a site.

Configuration Manager client computers cannot be automatically assigned to a site if any of the following apply, and then they must be manually assigned:

- They are currently assigned to a site.
- They are on the Internet or configured as Internet-only clients.
- Their network location does not fall within one of the configured boundary groups in the Configuration Manager hierarchy, and there is no fallback site for the hierarchy.

Completing Site Assignment by Checking Site Compatibility

After a client has found its assigned site, the version and operating system of the client is checked to ensure that a Configuration Manager site can manage it. For example, Configuration Manager cannot manage Configuration Manager 2007 clients, System Center 2012 Configuration Manager clients, or clients that are running Windows 2000.

Site assignment fails if you assign a client that runs Windows 2000 to a Configuration Manager site. When you assign a Configuration Manager 2007 client or a System Center 2012 Configuration Manager client to a Configuration Manager (current branch) site, site assignment succeeds to support automatic client upgrade. However, until the older generation clients are upgraded to a Configuration Manager (current branch) client, Configuration Manager cannot manage this client by using client settings, applications, or software updates.

> **NOTE**
> To support the site assignment of a Configuration Manager 2007 or a System Center 2012 Configuration Manager client to a Configuration Manager (current branch) site, you must configure automatic client upgrade for the hierarchy. For more information, see the How to upgrade clients for Windows computers in System Center Configuration Manager.

Configuration Manager also checks that you have assigned the Configuration Manager (current branch) client to a site that supports it. The following scenarios might occur during migration from previous versions of Configuration Manager.

- Scenario: You have used automatic site assignment and your boundaries overlap with those defined in a previous version of Configuration Manager.

  In this case, the client automatically tries to find a Configuration Manager (current branch) site.

  The client first checks Active Directory Domain Services and if it finds a Configuration Manager (current branch) site published, site assignment succeeds. If this fails (for example, the Configuration Manager site is not published or the computer is a workgroup client), the client then checks for site information from its assigned management point.

  > **NOTE**
  > You can assign a management point to the client during client installation by using the Client.msi property **SMSMP=<server_name>**.

  If both these methods fail, site assignment fails and you must manually assign the client.

- Scenario: You have assigned the Configuration Manager (current branch) client by using a specific site code rather than automatic site assignment, and mistakenly specified a site code for a version of Configuration Manager earlier than System Center 2012 R2 Configuration Manager.

  In this case, site assignment fails and you must manually reassign the client to a Configuration Manager (current branch) site.

  The site compatibility check requires one of the following conditions:

- The client can access site information published to Active Directory Domain Services.
- The client can communicate with a management point in the site.

  If the site compatibility check fails to finish successfully, the site assignment fails, and the client remains unmanaged until the site compatibility check runs again and succeeds.

  The exception to performing the site compatibility check occurs when a client is configured for an Internet-

based management point. In this case, no site compatibility check is made. If you are assigning clients to a site that contains Internet-based site systems, and you specify an Internet-based management point, ensure that you are assigning the client to the correct site. If you mistakenly assign the client to a Configuration Manager 2007 site, a System Center 2012 Configuration Manager site, or to a Configuration Manager site that does not have Internet-based site system roles, the client will be unmanaged.

Locating Management Points

After a client is successfully assigned to a site, it locates a management point in the site.

Client computers download a list of management points that they can connect to in the site. This happens whenever the client restarts, or every 25 hours, or if the client detects a network change, such as the computer disconnects and reconnects on the network or it receives a new IP address. The list includes management points on the intranet and whether they accept client connections over HTTP or HTTPS. When the client computer is on the Internet and the client doesn't yet have a list of management points, it connects to the specified Internet-based management point to obtain a list of management points. When the client has a list of management points for its assigned site, it then selects one to connect to:

- When the client is on the intranet and it has a valid PKI certificate that it can use, the client chooses HTTPS management points before HTTP management points. It then locates the closest management point, based on its forest membership.
- When the client is on the Internet, it randomly chooses one of the Internet-based management points.

Mobile device clients that are enrolled by Configuration Manager only connect to one management point in their assigned site and never connect to management points in secondary sites. These clients always connect over HTTPS and the management point must be configured to accept client connections over the Internet. When there is more than one management point for mobile device clients in the primary site, Configuration Manager randomly chooses one of these management points during assignment and the mobile device client continues to use the same management point.

When the client has downloaded client policy from a management point in the site, the client is then a managed client.

Downloading Site Settings

After site assignment succeeds, and the client has found a management point, a client computer that uses Active Directory Domain Services for its site compatibility check downloads client-related site settings for its assigned site. These settings include the client certificate selection criteria, whether to use a certificate revocation list, and the client request port numbers. The client continues to check these settings on a periodic basis.

When client computers cannot obtain site settings from Active Directory Domain Services, they download them from their management point. Client computers can also obtain the site settings when they are installed by using client push, or you can specify them manually by using CCMSetup.exe and client installation properties. For more information about the client installation properties, see About client installation properties in System Center Configuration Manager.

Downloading Client Settings

All clients download the default client settings policy and any applicable custom client settings policy. Software Center relies on these client configuration policies for Windows computers and will notify users that Software Center cannot run successfully until this configuration information is downloaded. Depending on the client settings that are configured, the initial download of client settings might take a while, and some client management tasks might not run until this process is complete.

Verifying Site Assignment

You can verify site assignment success by any of the following methods:

- For clients on Windows computers, use Configuration Manager in the Control Panel and verify that the site code is correctly displayed on the **Site** tab.
- For client computers, in the **Assets and Compliance** workspace > **Devices** node, verify that the computer displays **Yes** for the **Client** column and the correct primary site code for the **Site Code** column.
- For mobile device clients, in the **Assets and Compliance** workspace, use the **All Mobile Devices** collection to verify that the mobile device displays **Yes** for the **Client** column and the correct primary site code for the **Site Code** column.
- Use the reports for client assignment and mobile device enrollment.
- For client computers, use the LocationServices.log file on the client.

Roaming to Other Sites

When client computers on the intranet are assigned to a primary site but change their network location so that it falls within a boundary group that is configured for another site, they have roamed to another site. When this site is a secondary site for their assigned site, clients can use a management point in the secondary to download client policy and upload client data, which avoids sending this data over a potentially slow network. However, if these clients roam into the boundaries for another primary site or a secondary that is not a child site of their assigned site, these clients always use a management point in their assigned site to download client policy and to upload data to their site.

These client computers that roam to other sites (all primary sites and all secondary sites) can always use management points in other sites for content location requests. Management points in the current site can give clients a list of distribution points that have the content that clients request.

For client computers that are configured for Internet-only client management, and for mobile devices and Mac computers that are enrolled by Configuration Manager, these clients only communicate with management points in their assigned site. These clients never communicate with management points in secondary sites or with management points in other primary sites.

How to configure client status in System Center Configuration Manager

2/12/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Before you can monitor System Center Configuration Manager client status and remediate problems that are found, you must configure your site to specify the parameters that are used to mark clients as inactive and configure options to alert you if client activity falls below a specified threshold. You can also disable computers from automatically remediating any problems that client status finds.

To Configure Client Status

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, click **Client Status**, then, in the **Home** tab, in the **Client Status** group, click **Client Status Settings**.
3. In the **Client Status Settings Properties** dialog box, specify the following values to determine client activity:

   > **NOTE**
   > If none of the settings are met, the client will be marked as inactive.

   - **Client policy requests during the following days:** Specify the number of days since a client requested policy. The default value is **7** days.
   - **Heartbeat discovery during the following days:** Specify the number of days since the client computer sent a heartbeat discovery record to the site database. The default value is **7** days.
   - **Hardware inventory during the following days:** Specify the number of days since the client computer has sent a hardware inventory record to the site database. The default value is **7** days.
   - **Software inventory during the following days:** Specify the number of days since the client computer has sent a software inventory record to the site database. The default value is **7** days.
   - **Status messages during the following days:** Specify the number of days since the client computer has sent status messages to the site database. The default value is **7** days.
4. In the **Client Status Settings Properties** dialog box, specify the following value to determine how long client status history data is retained:
   - **Retain client status history for the following number of days:** Specify how long you want the client status history to remain in the site database. The default value is **31** days.
5. Click **OK** to save the properties and to close the **Client Status Settings Properties** dialog box.

To Configure the Schedule for Client Status

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, click **Client Status**, then, in the **Home** tab, in the **Client Status** group, click

Schedule Client Status Update.

3. In the **Schedule Client Status Update** dialog box, configure the interval at which you want client status to update and then click OK.

> **NOTE**
> When you change the schedule for client status updates, the update will not take effect until the next scheduled client status update (for the previously configured schedule).

To Configure Alerts for Client Status

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Device Collections**.
3. In the **Device Collections** list, select the collection for which you want to configure alerts and then, in the **Home** tab, in the **Properties** group, click **Properties**.

> **NOTE**
> You cannot configure alerts for user collections.

4. On the **Alerts** tab of the <*collection Name*>**Properties** dialog box, click **Add**.

> **NOTE**
> The **Alerts** tab is only visible if the security role you are associated with has permissions for alerts.

5. In the **Add New Collection Alerts** dialog box, choose the alerts that you want generated when client status thresholds fall below a specific value, then click **OK**.
6. In the **Conditions** list of the **Alerts** tab, select each client status alert and then specify the following information.
   - **Alert Name** - Accept the default name or enter a new name for the alert.
   - **Alert Severity** - From the drop-down list, choose the alert level that will be displayed in the Configuration Manager console.
   - **Raise alert** - Specify the threshold percentage for the alert.
7. Click **OK** to close the <*collection Name*>**Properties** dialog box.

To Exclude Computers from Automatic Remediation

1. Open the registry editor on the client computer for which you want to disable automatic remediation.

> **WARNING**
> If you use the Registry Editor incorrectly, you might cause serious problems that could require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using the Registry Editor incorrectly. Use the Registry Editor at your own risk.

2. Navigate to **HKEY_LOCAL_MACHINE\Software\Microsoft\CCM\CcmEval\NotifyOnly**.

3. Enter one of the following values for this registry key:

   - **True** - The client computer will not automatically remediate any problems that are found. However, you will still be alerted in the **Monitoring** workspace about any problems with this client.
   - **False** - The client computer will automatically remediate problems when they are found and you will be alerted in the **Monitoring** workspace. This is the default setting.

4. Close the registry editor.

   You can also install clients using the CCMSetup **NotifyOnly** installation property to exclude them from automatic remediation. For more information about this client installation property, see About client installation properties in System Center Configuration Manager.

How to monitor client deployment status in System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Deploying clients across your site takes time and some installations are not successful the first time. The System Center Configuration Manager console provides a way to keep an eye on client deployments within a collection by reporting client deployment status in real time.

> **NOTE**
> The best and most reliable way to monitor client deployment is with the Configuration Manager console (as described in this article). The **Client Status** section of the **Monitoring** workspace in the console provides client deployment status accurately and in real time. You can monitor client deployments with other tools, such as Server Manager in Windows Server or System Center Operations Manager, but you may receive alarms from normal client installation activity. Because of how the client installation program (CCMSetup.exe) runs in various environments, these other tools may generate false alarms and warnings that do not accurately reflect the state of client deployments.

In the **Monitoring** workspace of the console, you can monitor the following statuses for client deployments taking place within a collection that you specify:

- Compliant
- In progress
- Not compliant
- Failed
- Unknown

  Configuration Manager reports on deployments for production clients or pre-production clients. The Configuration Manager console also provides a chart of failed client deployments over a specified period of time to help you determine if actions you to take to troubleshoot deployments are improving the deployment success rate over time.

To monitor client deployments

- In the Configuration Manager console, click **Monitoring** > **Client Status**.
- Click **Production Client Deployment** or **Pre-production Client Deployment** depending on the version of client you want to monitor.
- Review the charts of client deployment status and client deployment failure.
- If you want to change the scope of the report, click **Browse...** and choose a different collection.

  To learn more about pre-production client deployments, see How to test client upgrades in a pre-production collection in System Center Configuration Manager.

> **NOTE**
>
> The deployment status on computers hosting site system roles in a pre-production collection may be reported as **Not compliant** even when the client was successfully deployed. When you promote the client to production, the deployment status is reported correctly.

To monitor the status of deployed clients, see How to monitor clients in System Center Configuration Manager

You can use Configuration Manager reports to find out more information about the status of clients in your site. For more information about how to run reports, see Reporting in System Center Configuration Manager.

Monitor and manage clients in Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

After you install the client on devices in your organization, Configuration Manager provides several ways to monitor and manage it. You can monitor clients to check their status, and Configuration Manager can automatically fix some problems it detects. Use the Configuration Manager console to manage clients for individual devices or device collections.

- How to monitor clients
- How to manage clients
- Manage clients on the internet
- Use collections

Co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune. It lets you cloud-attach your existing investment in Configuration Manager by adding new functionality. When you enable co-management, you can use Intune for additional client management actions. For more information, see What is co-management?.

How to monitor clients in Configuration Manager

7/15/2019 • 10 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Once you install the Configuration Manager client on the Windows devices in your site, monitor their health and activity in the Configuration Manager console.

About client status

Configuration Manager provides the following types of information as client status:

- **Client online status**: The site considers a device as **online** if it's connected to its assigned management point. To indicate that the client is online, it sends ping-like messages to the management point. If the management point doesn't receive a message in five minutes, the site considers the client as **offline**.
- **Client activity**: The site considers the client as **active** if it has communicated with Configuration Manager in the past seven days. The site considers the client **inactive** if it hasn't requested done the following actions in seven days:
  - Requested policy update
  - Sent a heartbeat message
  - Sent hardware inventory
- **Client check**: The state of the periodic evaluation that the Configuration Manager client runs on the device. The evaluation checks the device and can remediate some of the problems it finds. For more information, see Client health checks.

  On devices that run Windows 7, client check runs as a scheduled task. On later OS versions, client check runs automatically during the Windows maintenance window.

  You can configure remediation not to run on specific devices, for example, a business-critical server. If there are additional items that you want to evaluate, use Configuration Manager compliance settings to monitor additional configurations. For more information about compliance settings, see Plan for and configure compliance settings.
- **Decommissioned**: The site has marked the device record for deletion. This behavior can happen when a new registration for same device assigns to the same or a different primary site in a hierarchy. The site deletes these devices the next time it runs the site maintenance task **Delete Aged Discovery Data**.
- **Obsolete**: The site has discovered a new device record with the same hardware ID, so it marks the old record as obsolete. Reports don't count obsolete records of the same device multiple times. You can still target policies to obsolete devices. If the site doesn't get a heartbeat for an obsolete record after 90 days of inactivity, it removes the obsolete device when it runs the site maintenance task **Delete Obsolete Client Discovery Data**.

Monitor individual clients

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace. Select either the **Devices** node or choose a collection under **Device Collections**.

   The icons at the beginning of each row indicate the online status of the device:

	Device is online
	Device is offline
	Online status is unknown
	Client isn't installed on the device

2. For more detailed online status, add the client online status information to the device view. Right-click the column header and select the online status fields you want to add:

   - **Device Online Status**: Indicates whether the client is currently online or offline. (This status is the same information given by the icons.)
   - **Last Online Time**: Indicates when the client online status changed to online
   - **Last Offline Time** indicates when the status changed to offline

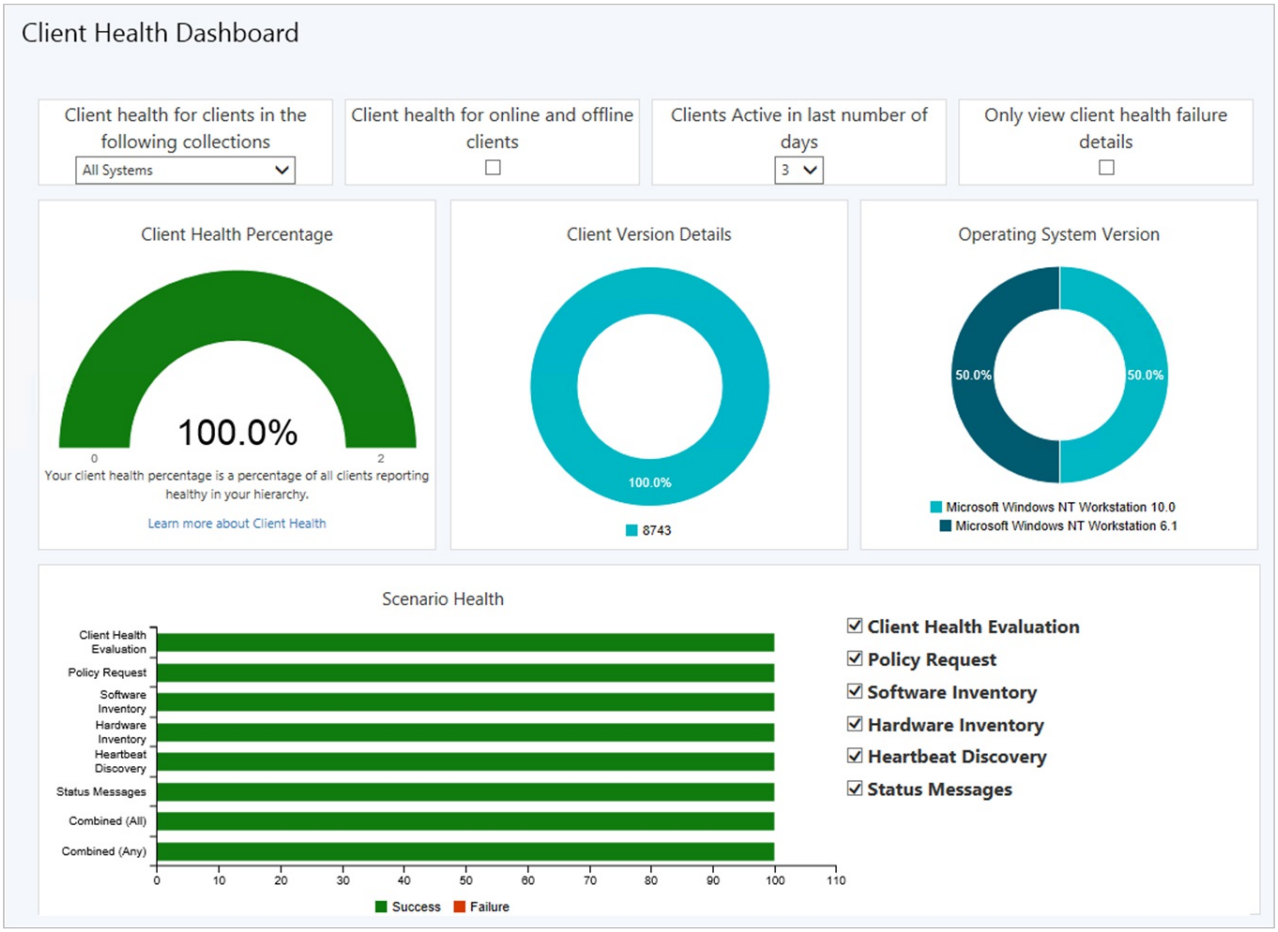
3. Select an individual client in the list pane to see more status in the detail pane. This information includes client activity and client check status.

Client health dashboard

You deploy software updates and other apps to help secure your environment, but these deployments only reach healthy clients. Unhealthy Configuration Manager clients adversely effect overall compliance. Determining client health can be challenging depending upon the denominator: how many total devices should be in your scope of management? For example, if you discover all systems from Active Directory, even if some of those records are for retired machines, this process increases your denominator.

Starting in version 1902, view a dashboard with information about the health of Configuration Manager clients in your environment. View your client health, scenario health, and common errors. Filter the view by several attributes to see any potential issues by OS and client versions.

In the Configuration Manager console, go to the **Monitoring** workspace. Expand **Client status**, and select the **Client health dashboard** node.



> **TIP**
>
> There are no changes to ccmeval.

By default, the client health dashboard shows online clients, and clients active in the past three days. Therefore, you may see different numbers in this dashboard than in other historical sources of client health. For example, other nodes under **Client Status**, or reports in the client status category.

Filters

At the top of the dashboard, there's a set of filters to adjust the data displayed in the dashboard.

- **Collection**: By default, the dashboard displays devices in the **All Systems** collection. Select a device collection from the list to scope the view to a subset of devices in a specific collection.
- **Online/offline**: By default, the dashboard displays only online clients. This state comes from the client notification channel that update a client's status every five minutes. For more information, see About client status.
- **Active # days**: By default, the dashboard displays clients that are active in the last three days.
- **Failure only**: Scope the view to only devices that are reporting a client health failure.

  > **TIP**
  >
  > Use this filter along with the client version and OS version tiles. For more information, see Version tiles.

Client health percentage

This tile shows the overall client health in your hierarchy.

A healthy Configuration Manager client has the following properties:

- Online
- Actively sending data
- Passes all client health evaluation checks

For more information, see About client status.

A healthy client successfully communicates with the site. It reports all data based on the defined schedules in client settings.

Select a segment of this chart to drill down to a device list view.

Version tiles

There are two tiles that show client health by Configuration Manager client version and OS version. These tiles are useful when you make changes to the filters, such as **Failure only**. They can help highlight whether any issues are consistent across a specific version. Use this information to help you make upgrade decisions.

Select a segment of these charts to drill down to a device list view.

Scenario health

This bar chart shows the overall health for the following core scenarios:

- Client policy
- Heartbeat discovery
- Hardware inventory
- Software inventory
- Status messages

Use the selectors to adjust the focus on specific scenarios in the chart.

The following two bars are always shown:

- **Combined (All)**: the combination of all scenarios (AND)
- **Combined (Any)**: at least one of the scenarios (OR)

> **TIP**
> Scenario health isn't measured from your configuration of client settings. These values can vary based upon the resultant set of policy per device. Use the following steps to adjust the evaluation periods for scenario health:
>
> - In the Configuration Manager console, go to the **Monitoring** workspace, and select the **Client Status** node.
> - In the ribbon, select **Client Status Settings**.
>
> By default, if a client doesn't send scenario-specific data in **7 days**, Configuration Manager considers it unhealthy for that scenario.

Top 10 client health failures

This chart lists the most common failures in your environment. These errors come from Windows or Configuration Manager.

Monitor the status of all clients

1. In the Configuration Manager console, go to the **Monitoring** workspace, and select the **Client Status** node. Review the overall statistics for client activity and client checks across the site. Change the scope of the information by choosing a different collection.

2. To drill down into detail about the reported statistics, choose the name of the reported information. For

example, **Active clients that have passed client check or no results**. Then review the information about the individual clients.

3. Select **Client Activity** to see charts showing the client activity in your Configuration Manager site.
4. Select **Client Check** to see charts showing the status of client checks in your Configuration Manager site.

   Configure alerts to notify you when client check results or client activity drops below a specified percentage. The site can also alert you when remediation fails on a specified percentage of clients. For more information, see How to configure client status.

Client health checks

Client check runs the following checks and remediations:

CLIENT CHECK	REMEDIATION ACTION	MORE INFORMATION
Verify that client check has recently run	Run client check	Checks that client check has run at least one time in the past three days.
Verify that client prerequisites are installed	Install the client prerequisites	Checks that client prerequisites are installed. Reads the file ccmsetup.xml in the client installation folder to discover the prerequisites.
WMI repository integrity test	Reinstall the Configuration Manager client	Checks that Configuration Manager client entries are present in WMI.
Verify that the client service is running	Start the client (SMS Agent Host) service	No additional information
WMI Event Sink Test.	Restart the client service	Check whether the Configuration Manager related WMI event sink is lost
Verify that the Windows Management Instrumentation (WMI) service exists	No remediation	No additional information
Verify that the client was installed correctly	Reinstall the client	No additional information
Verify that the antimalware service startup type is automatic	Reset the service startup type to automatic	No additional information
Verify that the antimalware service is running	Start the antimalware service	No additional information
Verify that the Windows Update service startup type is automatic or manual	Reset the service startup type to automatic	No additional information
Verify that the client service (SMS Agent Host) startup type is automatic	Reset the service startup type to automatic	No additional information
Verify that the Windows Management Instrumentation (WMI) service is running.	Start the Windows Management Instrumentation service	No additional information

CLIENT CHECK	REMEDIATION ACTION	MORE INFORMATION
Verify that the Microsoft SQL CE database is healthy	Reinstall the Configuration Manager client	No additional information
Microsoft Policy Platform WMI Integrity Test	Repair the Microsoft Policy Platform	No additional information
Verify that the Microsoft Policy Platform Service exists	Repair the Microsoft Policy Platform	No additional information
Verify that the Microsoft Policy Platform service startup type is manual	Reset the service startup type to manual	No additional information
Verify that the Background Intelligent Transfer Service exists	No Remediation	No additional information
Verify that the Background Intelligent Transfer Service startup type is automatic or manual	Reset the service startup type to automatic	No additional information
Verify that the Network Inspection Service startup type is manual	Reset the service startup type to manual if installed	No additional information
Verify that the Windows Management Instrumentation (WMI) service startup type is automatic	Reset the service startup type to automatic	No additional information
Verify that the Windows Update service startup type on Windows 8 devices is automatic or manual	Reset the service startup type to manual	No additional information
Verify that the client (SMS Agent Host) service exists.	No Remediation	No additional information
Verify that the Configuration Manager Remote Control service startup type is automatic or manual	Reset the service startup type to automatic	No additional information
Verify that the Configuration Manager Remote Control service is running	Start the remote control service	No additional information
Verify that the wake-up proxy service (ConfigMgr Wake-up Proxy) is running	Start the ConfigMgr Wakeup Proxy service	This client check is made only if the **Power Management**: **Enable wake-up proxy** client setting is set to **Yes** on supported client operating systems.
Verify that the wake-up proxy service (ConfigMgr Wake-up Proxy) startup type is automatic	Reset the ConfigMgr Wakeup Proxy service startup type to automatic	This client check is made only if the **Power Management**: **Enable wake-up proxy** client setting is set to **Yes** on supported client operating systems.

Client deployment log files

For more information about the log files used by client deployment and management operations, see Log files.

Use Windows Analytics with Configuration Manager

6/20/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Windows Analytics is a set of solutions that allow you to gain insight into the current state of your environment. Windows devices in your environment report data to Microsoft, which you can access and analyze through these solutions. For example, connect Upgrade Readiness to Configuration Manager to directly access the data in the **Monitoring** workspace of the Configuration Manager console.

The data used by Windows Analytics isn't transferred directly to the Configuration Manager site server. Client computers send data to the Windows cloud service. This service then transfers the relevant data to Windows Analytics solutions hosted in one of your organization's workspaces. Configuration Manager then directs you to relevant data in the web portal with in-context links. It can also directly display data that's part of solutions that you connect to Configuration Manager.

> **IMPORTANT**
> Configuration Manager reports diagnostics and usage data to Microsoft. This data is separate from Windows Analytics data. For more information, see Diagnostics and usage data.

Configure Clients to report data to Windows Analytics

For client devices to report data to Windows Analytics, configure them with a *commercial ID key*. This key is Azure Log Analytics workspace that hosts your Windows Analytics data. Also configure devices to report data at a level appropriate for the specific solutions that you want to use.

Configure Windows Analytics client settings

To configure Windows Analytics:

1. In the Configuration Manager console, go to the **Administration** workspace, and select the **Client Settings** node.
2. In the ribbon, select **Create Custom Device Client Settings**.
3. Add the **Windows Analytics** group to this custom device client settings policy.

For more information on creating custom device client settings, see How to configure client settings.

Select the **Windows Analytics** settings tab, and configure the following settings:

Manage Windows telemetry settings with Configuration Manager

Configure this setting to **Yes** to configure Windows diagnostic data settings on Windows clients.

Commercial ID key

The commercial ID key maps information from devices you manage to the Log Analytics workspace that hosts your organization's Windows Analytics data. If you've already configured a commercial ID key for use with Upgrade Readiness, use that ID. If you don't yet have a commercial ID key, see Copy your commercial ID key.

Windows 10 telemetry

For more information, see Configure Windows diagnostic data in your organization.

> **NOTE**
>
> You can also set the Windows 10 data collection level to **Enhanced (Limited)**. This setting enables you to gain actionable insight about devices in your environment without devices reporting all of the data in the **Enhanced** level with Windows 10 version 1709 or later. The Enhanced (Limited) level includes metrics from the Basic level, as well as a subset of data collected from the Enhanced level relevant to Windows Analytics.

Windows 8.1 and earlier telemetry

For more information, see Windows 7, Windows 8, and Windows 8.1 appraiser telemetry events and fields.

Enable Windows 8.1 and earlier Internet Explorer data collection

On devices running Windows 8.1 or earlier, Internet Explorer can collect data about web apps. This data can allow Upgrade Readiness to detect web application incompatibilities that could prevent a smooth upgrade to Windows 10. Enable Internet Explorer data collection based on the internet zone. For more information about internet zones, see About URL Security Zones.

Use Upgrade Readiness to identify Windows 10 compatibility issues

Upgrade Readiness enables you to analyze device readiness and compatibility with Windows 10. This assessment allows for smoother upgrades. After connecting Configuration Manager to Upgrade Readiness, access this client upgrade compatibility data directly in the Configuration Manager console. Then target devices for upgrade or remediation from the device list.

For more information and details on how to configure and connect to Upgrade Readiness, see Upgrade Readiness.

Use Windows Analytics to identify gaps in Windows Information Protection Policies

You can configure Windows 10 version 1703 and later devices with a Windows Information Protection (WIP) policy. They report diagnostic data on applications that access corporate data in your environment but aren't included in the policy application rules. Users may need these applications to stay productive, but WIP blocks the users' access. This information is useful to maintain your Windows Information Protection policies in Configuration Manager.

Integrate Upgrade Readiness with Configuration Manager

6/20/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Upgrade Readiness is a part of Windows Analytics. It allows you to assess and analyze the readiness of devices in your environment for an upgrade to Windows 10. Integrate Upgrade Readiness with Configuration Manager to access client upgrade compatibility data in the Configuration Manager console. Then use this data to create collections, and target devices for upgrade or remediation.

Configure clients

Upgrade Readiness relies on Windows Analytics data. In order for Upgrade Readiness to receive sufficient data, configure the following prerequisites:

- Configure all clients with a *commercial ID key*
- Configure Windows 10 clients for Windows Analytics to report at least basic level data
- For clients running Windows 7 or 8.1:
  - Install the updates as described in Get started with Upgrade Readiness
  - Enable Windows Analytics client settings

Configure these settings using Configuration Manager client settings. For more information, see Use Windows Analytics.

> **NOTE**
> Deploying the correct prerequisite updates and configuring client settings should be sufficient in most environments. If you encounter issues with Upgrade Readiness not receiving data from devices in your environment, then some of these issues may be addressed by using the Upgrade Readiness deployment script.

Connect Configuration Manager to Upgrade Readiness

Use the Azure services wizard to simplify the process of configuring Azure services you use with Configuration Manager. To connect Configuration Manager with Upgrade Readiness, create an Azure Active Directory (Azure AD) app registration of type *Web app / API* in the Azure portal. For more information about how to create an app registration, see Register your application with your Azure AD tenant.

In the Azure portal, give following permissions to your newly registered web app:

- *Reader* permissions to the resource group that contains the Log Analytics workspace with your Upgrade Readiness data
- *Contributor* permissions to the Log Analytics workspace that hosts your Upgrade Readiness data

The Azure services wizard uses this app registration to allow Configuration Manager to communicate securely with Azure AD and connect your infrastructure to your Upgrade Readiness data.

IMPORTANT

Grant permissions to the app itself, not to an Azure AD user identity. It's the registered app that accesses the data on behalf of your Configuration Manager infrastructure. To grant the permissions, search for the name of the app registration in the **Add users** area when assigning the permission.

This process is the same as when providing Configuration Manager with permissions to Log Analytics. These steps must be completed before the app registration is imported into Configuration Manager with the *Azure services wizard*.

For more information, see Connect Configuration Manager to Log Analytics.

Use the Azure Wizard to create the connection

Follow the instructions in Configure Azure services to create a connection to Upgrade Readiness by importing the web app registration you created above.

If the web app import was successful and the correct permissions are assigned in the Azure portal, the *Configuration* page pre-populates the following values:

- Azure subscriptions
- Azure resource group
- Windows Analytics workspace

More than one resource group or workspace is available in the following circumstances:

- If the registered Azure AD web app has *Contributor* permissions on more than one resource group
- If the selected resource group has more than one Log Analytics workspace

View and use Upgrade Readiness information in Configuration Manager

After you've integrated Upgrade Readiness with Configuration Manager, you can view the analysis of your clients' upgrade readiness.

1. In the Configuration Manager console, go to the **Monitoring** workspace, and select the **Upgrade Readiness** node.
2. Review the data. For example:
   - The upgrade readiness state
   - The percent of Windows devices that are reporting data
3. Filter the dashboard to view data for devices in specific collections.
4. View the devices in a particular readiness state, and then create a dynamic collection for those devices. Then use that collection to upgrade those devices, or take action to remediate devices that are in a blocked state.

NOTE

The site synchronizes data with Upgrade Readiness once a week. To manually trigger synchronization:

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Cloud Services**, and select the **Azure Services** node.
2. Select the Upgrade Readiness connection from the list.
3. In the ribbon, select the option to synchronize.

Next steps

- Upgrade Windows to the latest version
- Create a task sequence to upgrade an OS
- Create phased deployments

How to monitor clients for Linux and UNIX servers in Configuration Manager

3/27/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

> **IMPORTANT**
>
> Starting in version 1902, Configuration Manager doesn't support Linux or UNIX clients.
>
> Consider Microsoft Azure Management for managing Linux servers. Azure solutions have extensive Linux support that in most cases exceed Configuration Manager functionality, including end-to-end patch management for Linux.

You can view information from Linux and UNIX servers in the Configuration Manager console using the same methods you use to view information from Windows-based clients.

The information you can view includes:

- Status details from clients, in the Configuration Manager console dashboards
- Details about clients in the default Configuration Manager reports
- Inventory details in the Resource Explorer

  The following sections describe how to get these details from the resource explorer and reports.

Use resource explorer to view inventory for Linux and UNIX servers

After a Configuration Manager client submits hardware inventory to the Configuration Manager site, you can use Resource Explorer to view this information. The Configuration Manager client for Linux and UNIX doesn't add new classes or views for inventory to the Resource Explorer. The Linux and UNIX inventory data maps to existing WMI classes. You can view the inventory details for your Linux and UNIX servers in the Windows-based classifications using Resource Explorer.

For example, you can collect the list of all natively installed programs found on your Linux and UNIX servers. Examples of natively installed programs include **.rpms** in Linux or **.pkgs** in Solaris. After inventory has been submitted by a Linux or UNIX client, you can view the list of all the natively installed Linux or UNIX programs in Resource Explorer in the Configuration Manager console.

For information about how to use Resource Explorer, see How to use Resource Explorer to view hardware inventory in System Center Configuration Manager.

How to use Reports to View Information for Linux and UNIX Servers

Reports for Configuration Manager include information from Linux and UNIX servers along with information from Windows-based computers. No additional configurations are required to integrate the Linux and UNIX data in the reports.

For example, if you run the report named Count of Operating System Versions, it displays the list of the different operating systems and the number of clients that are running each operating system. The report is based on the hardware inventory information that was sent by the different Configuration Manager clients that run on the different operating systems.

It's also possible to create custom reports that are specific to Linux and UNIX server data. The **Caption** property of the hardware inventory class **Operating System** is a useful attribute that you can use to identify specific Operating Systems in the report query.

For information about reports in Configuration Manager, see Reporting in System Center Configuration Manager.

How to manage clients in Configuration Manager

9/6/2019 • 17 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

When the Configuration Manager client installs on a device and successfully assigns to a site, you see the device in the **Assets and Compliance** workspace in the **Devices** node, and in one or more collections in the **Device Collections** node. Select the device or a collection, and then run management operations. However, there are other ways to manage the client, which might involve other workspaces in the console, or tasks outside of the console.

> **NOTE**
>
> If you install the Configuration Manager client, but it hasn't yet successfully assigned to a site, it might not display in the console. After the client assigns to a site, update collection membership, and then refresh the console view.
>
> A device can also display in the console when the Configuration Manager client isn't installed. This behavior happens if the site discovers a device but the client isn't installed and assigned.
>
> Mobile devices managed with the Exchange Server connector or on-premises MDM don't install the Configuration Manager client.
>
> To manage a device from the console, use the **Client** column in the **Devices** node to determine whether the client is installed.

Manage clients from the **Devices** node

Depending on the device type, some of these options might not be available.

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace, and select the **Devices** node.
2. Select one or more devices, and then select one of these client management tasks from the ribbon. You can also right-click the device.)

Import user device affinity

Configure the associations between users and devices, so you can efficiently deploy software to users.

For more information, see Link users and devices with user device affinity.

Import computer information

Launch the **Import Computer Information Wizard** to import new computer information into the Configuration Manager database. You can import multiple computers using a file, or specify information for a single computer.

Add selected items

Provides the following options:

- **Add selected items to existing device collection**: Opens the **Select Collection** dialog box. Select the collection to which you want to add this device. The device is included in this collection by using a **Direct** membership rule.
- **Add selected items to new device collection**: Opens the **Create Device Collection Wizard** where you can create a new collection. The selected collection is included in this collection by using a **Direct**

membership rule.

For more information, see How to create collections.

Install client

Opens the **Install Client Wizard**. This wizard uses client push installation to install or reinstall the Configuration Manager client on the selected device.

> **TIP**
> There are many different ways to install the Configuration Manager client. Although the Client Push wizard offers a convenient client installation method from the console, this method has many dependencies and isn't suitable for all environments. For more information about the dependencies, see Prerequisites for deploying clients to Windows computers. For more information about the other client installation methods, see Client installation methods.

For more information, see How to install Configuration Manager clients by using client push.

Run script

Opens the **Run Script** wizard to run a PowerShell script on the selected device.

For more information, see Create and run PowerShell scripts.

Install application

Install an application to a device in real time. This feature can help reduce the need for separate collections for every application.

For more information, see Install applications for a device.

Reassign site

Reassign one or more clients, including managed mobile devices, to another primary site in the hierarchy. You can individually reassign clients or select more than one to reassign them in bulk.

Client settings - Resultant client settings

When you deploy multiple client settings to the same device, the prioritization and combination of settings is complex. Use this option to view the resultant set of client settings deployed to this device.

For more information, see How to configure client settings.

Start

- Run **Resource Explorer** to see the hardware and software inventory information from a Windows client. For more information, see the following articles:
  - How to use Resource Explorer to view hardware inventory
  - How to use Resource Explorer to view software inventory
- Remotely administer the device by using **Remote Control**, **Remote Assistance**, or **Remote Desktop Client**. For more information, see How to remotely administer a Windows client computer.

Approve

When the client communicates with site systems using HTTP and a self-signed certificate, you must approve these clients to identify them as trusted computers. By default, the site configuration automatically approves clients from the same Active Directory forest and trusted forests. This default behavior means that you don't have to manually approve each client. Manually approve workgroup computers that you trust, and any other unapproved computers that you trust.

> **IMPORTANT**
> Although some management functions might work for unapproved clients, this is an unsupported scenario for Configuration Manager.

You don't have to approve clients that always communicate to site systems using HTTPS, or clients that use a PKI certificate when they communicate to site systems using HTTP. These clients establish trust by using the PKI certificates.

Block or unblock

Block a client that you no longer trust. Blocking prevents the client from receiving policy, and prevents site systems from communicating with the client.

> **IMPORTANT**
> Blocking a client only prevents communication from the client to Configuration Manager site systems. It doesn't prevent communication to other devices. When the client communicates to site systems by using HTTP instead of HTTPS, there are some security limitations.

You can also unblock a client that is blocked.

For more information, ee Determine whether to block clients.

Clear required PXE deployments

You can redeploy a required PXE deployment by clearing the status of the last PXE deployment assigned to a Configuration Manager collection or a computer. This action resets the status of that deployment and reinstalls the most recent required deployments.

For more information, see Use PXE to deploy Windows over the network.

Client notification

For more information, see Client notifications.

Endpoint Protection

For more information, see Client notifications.

Edit primary users

View users of this device in the last 90 days, or specify the primary users of this device.

For more information, see Link users and devices with user device affinity.

Wipe a mobile device

You can wipe mobile devices that support the wipe command. This action permanently removes all data on the mobile device, including personal settings and personal data. Typically, this action resets the mobile device back to factory defaults. Wipe a mobile device when it's no longer trusted. For example, if the device is lost or stolen.

> **TIP**
> Check the manufacturer's documentation for more information about how the mobile device processes a remote wipe command.

There's often a delay until the mobile device receives the wipe command:

- If the mobile device is enrolled by Configuration Manager, the client receives the command when it downloads its client policy.

- If the mobile device is managed by the Exchange Server connector, it receives the command when it synchronizes with Exchange.

To monitor when the device receives the wipe command, use the **Wipe Status** column. Until the device sends a wipe acknowledgment to Configuration Manager, you can cancel the wipe command.

Retire a mobile device

The **Retire** option is supported only by mobile devices enrolled by on-premises MDM.

For more information, see Help protect your data with remote wipe, remote lock, or passcode reset.

Change ownership

If a device isn't domain-joined and doesn't have the Configuration Manager client installed, use this option to change the ownership to **Company** or **Personal**.

You can use this value in application requirements to control deployments, and to control how much inventory is collected from users' devices.

You may need to add the **Device Owner** column to the view by right-clicking any column heading and choosing it.

For more information, see Hybrid MDM with Configuration Manager and Microsoft Intune.

Delete

> **WARNING**
> Don't delete a client if you want to uninstall the Configuration Manager client or remove it from a collection.

The **Delete** action manually removes the client record from the Configuration Manager database. Only use this action to troubleshoot a problem. If you delete the object, but the client is still installed and communicating with the site, Heartbeat Discovery recreates the client record. It reappears in the Configuration Manager console, although the client history and any previous associations are lost.

> **NOTE**
> When you delete a mobile device client that was enrolled by Configuration Manager, this action also revokes the issued PKI certificate. This certificate is then rejected by the management point, even if IIS doesn't check the certificate revocation list (CRL).
>
> Certificates on mobile device legacy clients are not revoked when you delete these clients.

To uninstall the client, see Uninstall the Configuration Manager client.

To assign the client to a new primary site, see How to assign clients to a site.

To remove the client from a collection, reconfigure the collection properties. For more information, see How to manage collections.

Refresh

Refresh the console view with the latest data in the database. For example, if a device appears in the list from discovery, but doesn't show as installed. After you install the client and make sure it's assigned to the site, select **Refresh**.

Properties

View the discovery data and deployments targeted for the client.

You can also configure variables that task sequences use to deploy an OS to the device. For more information, se Create task sequence variables for computers and collections.

Manage clients from the **Device Collections** node

Many of the tasks that are available for devices in the **Devices** node are also available on collections. The console automatically applies the operation to all eligible devices in the collection. This action on an entire collection generates additional network packets and increases CPU usage on the site server.

Consider the following questions before you run collection-level tasks. Once started, you can't stop the task from the console.

- How many devices are in the collection?
- Are the devices connected by low-bandwidth network connections?
- How much time does this task need to complete for all the devices?

For more information, see How to manage collections.

Restart clients

Use the Configuration Manager console to identify clients that require a restart. Then use a client notification action to restart them.

> **TIP**
> Enable automatic client upgrade to keep your clients up-to-date with less effort. For more information, see About automatic client upgrade.

To identify devices that are pending a restart, go to the **Assets and Compliance** workspace in the Configuration Manager console and select the **Devices** node. Then view the status for each device in the details pane in a new column named **Pending Restart**. Each device has one or more of the following values:

- **No**: there's no pending restart
- **Configuration Manager**: this value comes from the client reboot coordinator component (RebootCoordinator.log)
- **File rename**: this value comes from Windows reporting a pending file rename operation (HKLM\SYSTEM\CurrentControlSet\Control\Session Manager, PendingFileRenameOperations)
- **Windows Update**: this value comes from the Windows Update Agent reporting a pending restart is required for one or more updates (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\RebootRequired)
- **Add or remove feature**: this value comes from the Windows component-based servicing reporting the addition or removal of a Windows feature requires a restart (HKLM\Software\Microsoft\Windows\CurrentVersion\Component Based Servicing\Reboot Pending)

Create the client notification to restart a device

1. Select the device you want to restart within a collection in the **Device Collections** node of the console.
2. In the ribbon, select **Client Notification**, and then select **Restart**. An information window opens about the restart. Select **OK** to confirm the restart request.

When the notification is received by a client, a **Software Center** notification window opens to inform the user about the restart. By default, the restart occurs after 90 minutes. You can modify the restart time by configuring client settings. Settings for the restart behavior are found on the Computer restart tab of the default settings.

Configure the client cache

The client cache stores temporary files for when clients install applications and programs. Software updates also use the client cache, but always attempt to download to the cache regardless of the size setting. Configure the cache settings, such as size and location, when you manually install the client, when you use client push installation, or after installation.

You can specify the cache folder size using client settings in the Configuration Manager console. For more information, see Client cache settings.

The default location for the Configuration Manager client cache is `%windir%\ccmcache` and the default disk space is 5120 MB.

> **IMPORTANT**
> Don't encrypt the folder used for the client cache. Configuration Manager can't download content to an encrypted folder.

About the client cache

The Configuration Manager client downloads the content for required software soon after it receives the deployment but waits to run it until the deployment scheduled time. At the scheduled time, the Configuration Manager client checks to see whether the content is available in the cache. If content is in the cache and it's the correct version, the client uses the cached content. When the required version of the content changes, or if the client deletes the content to make room for another package, the client downloads the content to the cache again.

If the client attempts to download content for a program or application that is greater than the size of the cache, the deployment fails because of insufficient cache size. The client generates status message 10050 for insufficient cache size. If you increase the cache size later, the result is:

- For a required program: The client doesn't automatically retry to download the content. Redeploy the package and program to the client.
- For a required application: The client automatically retries to download the content when it downloads its client policy.

If the client attempts to download a package that's less than the size of the cache, but the cache is full, all *required* deployments keep retrying until:

- The cache space is available
- The download times out
- The retry count reaches its limit

If you later increase the cache size, the client attempts to download the package again during the next retry interval. The client tries to download the content every four hours until it tries 18 times.

Cached content isn't automatically deleted. It remains in the cache for at least one day after the client uses that content. If you configure the package properties with the option to persist content in the client cache, the client doesn't automatically delete it. If the cache space is used by packages that were downloaded within the last 24 hours, and the client must download new packages, either increase the cache size or choose the option to delete persisted cache content.

Use the following procedures to configure the client cache during manual client installation, or after the client is installed.

Configure the cache during manual client installation

Run the CCMSetup.exe command from the install source location and specify the following properties that you require, and separated by spaces:

- DISABLECACHEOPT
  - SMSCACHEDIR
  - SMSCACHEFLAGS
  - SMSCACHESIZE

    > **NOTE**
    > Use the cache size settings available in **Client Settings** in the Configuration Manager console instead of SMSCACHESIZE. For more information, see Client cache settings.

For more information about how to use these command-line properties for CCMSetup.exe, see About client installation properties.

Configure the cache during client push installation

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. Select the appropriate site. On the **Home** tab of the ribbon, in the **Settings** group, select **Client Installation Settings**, and choose **Client Push Installation**. Switch to the **Installation Properties** tab.
3. Specify the following properties, separated by spaces:
   - DISABLECACHEOPT
   - SMSCACHEDIR
   - SMSCACHEFLAGS
   - SMSCACHESIZE

     > **NOTE**
     > Use the cache size settings available in **Client Settings** in the Configuration Manager console instead of SMSCACHESIZE. For more information, see Client cache settings.

     For more information about how to use these command-line properties for CCMSetup.exe, see About client installation properties.

Configure the cache on the client computer

1. On the client computer, open the **Configuration Manager** control panel.
2. Switch to the **Cache** tab. Set the space and location properties. The default location is `%windir%\ccmcache`.
3. To delete the files in the cache folder, choose **Delete Files**.

Configure client cache size in Client Settings

Adjust the size of the client cache without having to reinstall the client. Use the cache size settings available in **Client Settings** in the Configuration Manager console. For more information, see Client cache settings.

Uninstall the client

You can uninstall the Configuration Manager client software from a computer by using **CCMSetup.exe** with the **/Uninstall** property. Run CCMSetup.exe on an individual computer from the command prompt, or deploy a package to uninstall the client for a collection of computers.

> **NOTE**
> You can't uninstall the Configuration Manager client from a mobile device. If you must remove the Configuration Manager client from a mobile device, you must wipe the device, which deletes all data on the mobile device.

1. Open a Windows command prompt as an administrator. Change the folder to the location in which CCMSetup.exe is located, for example: `cd %windir%\ccmsetup`
2. Run the following command: `CCMSetup.exe /uninstall`

> **TIP**
> The uninstall process displays no results on the screen. To verify that the client successfully uninstalls, see the following log file: `%windir%\ccmsetup\logs\CCMSetup.log`
>
> If you need to wait for the uninstall process to complete before doing something else, run `Wait-Process CCMSetup` in PowerShell. This command can pause a script until the CCMSetup process completes.

Manage conflicting records

Configuration Manager uses the hardware identifier to attempt to identify clients that might be duplicates and alert you to the conflicting records. For example, if you reinstall a computer, the hardware identifier would be the same but the GUID used by Configuration Manager might be changed.

Configuration Manager automatically resolves conflicts by using Windows authentication of the computer account or a PKI certificate from a trusted source. When Configuration Manager can't resolve the conflict of duplicate hardware identifiers, a hierarchy setting determines the behavior.

Change the hierarchy setting for managing conflicting records

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. In the ribbon, select **Hierarchy Settings**.
3. Switch to the **Client Approval and Conflicting Records** tab, and select one of the following options:
   - **Automatically resolve conflicting records**
   - **Manually resolve conflicting records**

Manually resolve conflicting records

1. In the Configuration Manager console, go to the **Monitoring** workspace, expand **System Status**, and select the **Conflicting Records** node.
2. Select one or more conflicting records, and then choose **Conflicting Record**.
3. Select one of the following options:
   - **Merge**: Combine the newly detected record with the existing client record.
   - **New**: Create a new record for the conflicting client record.
   - **Block**: Create a new record for the conflicting client record, but mark it as blocked.

Manage duplicate hardware identifiers

You can provide a list of hardware identifiers that Configuration Manager ignores for PXE boot and client registration. This list helps to address two common issues:

1. Many new devices don't include an onboard Ethernet port. Technicians use a USB-to-Ethernet adapter to establish a wired connection for purposes of OS deployment. These adapters are often shared because of cost and general usability. The site uses the MAC address of this adapter to identify the device. So reusing the adapter becomes problematic without additional administrator actions between each deployment. To reuse the adapter in this scenario, exclude its MAC address.
2. While the SMBIOS attribute should be unique, some specialty hardware devices have duplicate identifiers. Exclude this duplicate identifier and rely on the unique MAC address of each device.

Use the following process to add hardware identifiers for Configuration Manager to ignore:

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Sites** node.
2. On the **Home** tab of the ribbon, in the **Sites** group, choose **Hierarchy Settings**.
3. Switch to the **Client Approval and Conflicting Records** tab. To add new hardware identifiers, choose **Add** in the **Duplicate hardware identifiers** section.

Start policy retrieval

A Configuration Manager client downloads its client policy on a schedule that you configure as a client setting. You can also start on-demand policy retrieval from the client. For example, for troubleshooting or testing situations.

- Client notification
- The client control panel
- Support Center
- A script

Start client policy retrieval with client notification

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace, and select **Devices**.
2. Select the device that you want to download policy. On the **Home** tab of the ribbon, in the **Device** group, select **Client Notification**, and then choose **Download Computer Policy**.

> **NOTE**
> You can also use client notification to start policy retrieval for all devices in a collection.

Start client policy retrieval from the Configuration Manager client control panel

1. Open the **Configuration Manager** control panel on the computer.
2. Switch to the **Actions** tab. Select **Machine Policy Retrieval & Evaluation Cycle** to start the computer policy, and then select **Run Now**.
3. Select **OK** to confirm the prompt.
4. Repeat the previous steps for any other actions. For example, **User Policy Retrieval & Evaluation Cycle** for user client settings.

Start client policy retrieval with Support Center

Use Support Center to request and view client policy. For more information, see Support Center reference.

Start client policy retrieval by script

1. Open a script editor, such as Notepad or Windows PowerShell ISE.

2. Copy and insert the following sample PowerShell code into the file:

```
$trigger = "{00000000-0000-0000-0000-000000000021}"
Invoke-WmiMethod -Namespace root\ccm -Class sms_client -Name TriggerSchedule $trigger
```

> **TIP**
>
> For more information about the schedule IDs, see Message IDs.

3. Save the file with a .ps1 extension.
4. Run the script on the client.

Client notification in Configuration Manager

9/6/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

To take immediate action on remote clients, send a client notification action from the Configuration Manager console. Start these actions on an individual device or on a collection of devices.

Actions

The following actions are on the ribbon in the Device or Collection group of the Home tab.

Install client

Opens the **Install Client Wizard**. This wizard uses client push installation to install a Configuration Manager client. For more information, see Client push installation.

Permissions

This action requires the **Modify Resource** and **Read** permissions on the **Collection** object.

The following built-in roles have these permissions by default:

- Application Administrator
- Full Administrator
- Infrastructure Administrator
- Operations Administrator
- OS Deployment Manager

Add these permissions to any custom roles that need to push the client.

Run script

Opens the **Run Script** wizard to run a PowerShell script on all of the clients in the collection. For more information, see Create and run PowerShell scripts.

Permissions

This action requires the **Run Script** permission on the **Collection** object.

The following built-in roles have this permission by default:

- Full Administrator
- Infrastructure Administrator
- Operations Administrator

Add this permission to any custom roles that need to run scripts.

Start CMPivot

Starts **CMPivot**, which runs real-time queries against the targeted devices. For more information, see CMPivot.

Permissions

This action requires the same permissions as the Run script action.

Client notification

These actions are under the **Client notification** menu, on the ribbon in the Device or Collection group of the

Home tab.

In version 1806 or earlier, the **Client Notification** option is only available from either the Device Collection node or when you viewed the membership of a Device Collection. Starting in version 1810, you can start a **Client Notification** directly from the **Devices** node. There's no longer a requirement to be within a collection membership view.

Permissions

Starting in version 1810, client notification actions now require the **Notify Resource** permission on the Collection object. This permission applies to all actions under the **Client notification** menu.

The following built-in roles have this permission by default:

- Full Administrator
- Infrastructure Administrator

Add this permission to any custom roles that need to use client notification actions.

Download computer policy

Refresh the device policy. For more information, see Initiate policy retrieval for a Configuration Manager client.

Download user policy

Refresh the user policy.

Collect discovery data

Trigger clients to send a discovery data record (DDR). For more information, see Heartbeat discovery.

Collect software inventory

Trigger clients to run a software inventory cycle. For more information, see Introduction to software inventory.

Collect hardware inventory

Trigger clients to run a hardware inventory cycle. For more information, see Introduction to hardware inventory.

Evaluate application deployments

Trigger clients to run an application deployment evaluation cycle. For more information, see Schedule re-evaluation for deployments.

Evaluate software update deployments

Trigger clients to run a software updates deployment evaluation cycle. For more information, see Introduction to software updates.

Switch to the next software update point

Trigger clients to switch to the next available software update point. For more information, see Software update point switching.

Evaluate device health attestation

Trigger Windows 10 clients to check and send their latest device health state. For more information, see Health attestation.

Check conditional access compliance

Trigger clients to check their compliance with conditional access. For more information, see Manage access to Office 365 services for PCs.

Wake Up

Starting in version 1810, trigger devices configured to support Wake-on-LAN to wake up using other devices on the same subnet to send the Wake-on-LAN package. For more information, see How to configure Wake on LAN.

Permissions

This action requires the **Notify resource** permission on the **Collection** object.

Restart

Trigger the selected devices to restart. For more information, see Restart clients.

Endpoint Protection

The following actions are under the **Endpoint Protection** menu. This menu is on the ribbon in the Collection group of the Home tab. When you select one or more devices, these actions are on the **Selected Object** tab of the ribbon.

For more information, see Endpoint Protection in Configuration Manager.

Permissions

This action requires the **Enforce Security** permission on the **Collection** object.

The following built-in roles have this permission by default:

- Full Administrator
- Endpoint Protection Manager
- Operations Administrator

Add this permission to any custom roles that need to trigger Endpoint Protection actions.

Full Scan

Trigger Endpoint Protection or Windows Defender to run a *full* antimalware scan.

Quick Scan

Trigger Endpoint Protection or Windows Defender to run a *quick* antimalware scan.

Download Definition

Trigger Endpoint Protection or Windows Defender to download the latest antimalware definitions.

See also

- How to manage clients
- How to manage collections

How to manage clients for Linux and UNIX servers in Configuration Manager

3/27/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

IMPORTANT

Starting in version 1902, Configuration Manager doesn't support Linux or UNIX clients.

Consider Microsoft Azure Management for managing Linux servers. Azure solutions have extensive Linux support that in most cases exceed Configuration Manager functionality, including end-to-end patch management for Linux.

When you manage Linux and UNIX servers with Configuration Manager, you can configure collections, maintenance windows, and client settings to help manage the servers. Also, though the Configuration Manager client for Linux and UNIX doesn't have a user interface, you can force the client to manually poll for client policy.

Collections of Linux and UNIX servers

Use collections to manage groups of Linux and UNIX servers in the same way you use collections to manage other client types. Collections can be direct membership collections or query-based collections. Query-based collections identify client operating systems, hardware configurations, or other details about the client that are stored in the site database. For example, you can use collections that include Linux and UNIX servers to manage the following settings:

- Client settings
- Software deployments
- Enforce maintenance windows

  Before you can identify a Linux or UNIX client by its operating system or distribution, you must collect hardware inventory from the client.

  The default client settings for hardware inventory include information about a client computer's operating system. You can use the **Caption** property of the **Operating System** class to identify the operating system of a Linux or UNIX server.

  You can view details about computers that run the Configuration Manager client for Linux and UNIX in the **Devices** node of the **Assets and Compliance** workspace in the Configuration Manager console. In the **Asset and Compliance** workspace of the Configuration Manager console, you can view the name of each computer's operating system in the **Operating System** column.

  By default, Linux and UNIX servers are members of the **All Systems** collection. We recommend that you build custom collections that include only Linux and UNIX servers, or a subset of them. Custom collections enable you to manage operations such as deploying software or assigning client settings to groups of like computers, so that you can accurately measure the success of a deployment.

  When you build a custom collection for Linux and UNIX servers, include membership rule queries that include the Caption attribute for the Operating System attribute. For information about creating collections, see How to create collections in System Center Configuration Manager.

Maintenance windows for Linux and UNIX servers

The Configuration Manager client for Linux and UNIX servers supports the use of maintenance windows. This support is unchanged from Windows-based clients.

Client settings for Linux and UNIX servers

You can configure client settings that apply to Linux and UNIX servers the same way you configure settings for other clients.

By default, the **Default Client Agent Settings** apply to Linux and UNIX servers. You can also create custom client settings and deploy them to collections of specific clients.

There are no additional client settings that apply only to Linux and UNIX clients. However, there are default client settings that don't apply to Linux and UNIX clients. The client for Linux and UNIX only applies settings for functionality that it supports.

For example, a custom client device setting that enables and configures remote control settings would be ignored by the Linux and UNIX servers, because the client for Linux and UNIX doesn't support remote control.

Computer policy for Linux and UNIX servers

The client for Linux and UNIX servers periodically polls its site for computer policy to learn about requested configurations and to check for deployments.

You can also force the client on a Linux or UNIX server to immediately poll for computer policy. To do so, use **root** credentials on the server to run the following command: **/opt/microsoft/configmgr/bin/ccmexec -rs policy**

Details about the computer policy poll are entered into the shared client log file, **scxcm.log**.

> **NOTE**
> The Configuration Manager client for Linux and UNIX never requests nor processes user policy.

How to manage certificates on the client for Linux and UNIX

After you install the client for Linux and UNIX, you can use the **certutil** tool to update the client with a new PKI certificate, and to import a new Certificate Revocation list (CRL). When you install the client for Linux and UNIX, this tool is placed in `/opt/microsoft/configmgr/bin/certutil`.

To manage certificates, on each client run certutil with one of the following options:

OPTION	MORE INFORMATION

OPTION	MORE INFORMATION
`importPFX`	Use this option to specify a certificate to replace the certificate that is currently used by a client. When you use `-importPFX`, you must also use the `-password` command-line parameter to supply the password associated with the PKCS#12 file. Use `-rootcerts` to specify any additional root certificate requirements. Example: `certutil -importPFX <path to the PKCS#12 certificate> -password <certificate password> [-rootcerts <comma-separated list of certificates>]`
`importsitecert`	Use this option to update the site server signing certificate that is on the management server. Example: `certutil -importsitecert <path to the DER certificate>`
`importcrl`	Use this option to update the CRL on the client with one or more CRL file paths. Example: `certutil -importcrl <comma separated CRL file paths>`

Maintain Mac clients

9/11/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Here are procedures for uninstalling Mac clients and for renewing their certificates.

Uninstalling the Mac client

1. On a Mac computer, open a terminal window and navigate to the folder containing **macclient.dmg**.
2. Navigate to the Tools folder and enter the following command-line:

   ```
   ./CMUninstall -c
   ```

   > **NOTE**
   > The **-c** property instructs the client uninstall to also remove client crash logs and log files. We recommend this to avoid confusion if you later reinstall the client.

3. If required, manually remove the client authentication certificate that Configuration Manager was using, or revoke it. CMUnistall does not remove or revoke this certificate.

Renewing the Mac client certificate

Use one of the following methods to renew the Mac client certificate:

- Renew certificate wizard
- Renew certificate manually

Renew certificate wizard

1. Configure the following values as *strings* in the ccmclient.plist file that controls when the Renew Certificate Wizard opens:

   - **RenewalPeriod1** - Specifies, in seconds, the first renewal period in which users can renew the certificate. The default value is 3,888,000 seconds (45 days). Don't configure a value less than 300, as the period will revert to the default.
   - **RenewalPeriod2** - Specifies, in seconds, the second renewal period in which users can renew the certificate. The default value is 259,200 seconds (3 days). If this value is configured and is greater than or equal to 300 seconds and is less than or equal to **RenewalPeriod1**, the value will be used. If **RenewalPeriod1** is greater than 3 days, a value of 3 days will be used for **RenewalPeriod2**. If **RenewalPeriod1** is less than 3 days, then **RenewalPeriod2** is set to the same value as **RenewalPeriod1**.
   - **RenewalReminderInterval1** - Specifies, in seconds, the frequency at which the Renew Certificate Wizard will be displayed to users during the first renewal period. The default value is 86,400 seconds (1 day). If **RenewalReminderInterval1** is greater than 300 seconds and less than the value configured for **RenewalPeriod1**, then the configured value will be used. Otherwise, the default value of 1 day will be used.
   - **RenewalReminderInterval2** - Specifies, in seconds the frequency at which the Renew Certificate

Wizard will be displayed to users during the second renewal period. The default value is 28,800 seconds (8 hours). If **RenewalReminderInterval2** is greater than 300 seconds, less than or equal to **RenewalReminderInterval1** and less than or equal to **RenewalPeriod2**, then the configured value will be used. Otherwise, a value of 8 hours will be used.

Example: If the values are left as their defaults, 45 days before the certificate expires, the wizard will open every 24 hours. Within 3 days of the certificate expiring, the wizard will open every 8 hours.

Example: Use the following command line, or a script, to set the first renewal period to 20 days.

```
sudo defaults write com.microsoft.ccmclient RenewalPeriod1 1728000
```

2. When the Renew Certificate Wizard opens, the **User name** and **Server name** fields will typically be pre-populated and the user can just enter a password to renew the certificate.

> **NOTE**
> If the wizard does not open, or if you accidentally close the wizard, click **Renew** from the **Configuration Manager** preference page to open the wizard.

Renew certificate manually

A typical validity period for the Mac client certificate is 1 year. Configuration Manager does not automatically renew the user certificate that it requests during enrollment, so you must use the following procedure to renew the certificate manually.

> **IMPORTANT**
> If the certificate expires, you must uninstall, reinstall and then re-enroll the Mac client.

This procedure removes the SMSID, which is required to request a new certificate for the same Mac computer. When you remove and replace the client SMSID, any stored client history such as inventory is deleted after you delete the client from the Configuration Manager console.

1. Create and populate a device collection for the Mac computers that must renew the user certificates.

> **WARNING**
> Configuration Manager does not monitor the validity period of the certificate that it enrolls for Mac computers. You must monitor this independently from Configuration Manager to identify the Mac computers to add to this collection.

2. In the **Assets and Compliance** workspace, start the **Create Configuration Item Wizard**.
3. On the **General** page, specify the following information:
   - **Name:Remove SMSID for Mac**
   - **Type:Mac OS X**
4. On the **Supported Platforms** page, ensure that all Mac OS X versions are selected.
5. On the **Settings** page, choose **New** and then, in the **Create Setting** dialog box, specify the following information:
   - **Name:Remove SMSID for Mac**
   - **Setting type:Script**

- **Data type:String**

6. In the **Create Setting** dialog box, for **Discovery script**, choose **Add script** to specify a script that discovers Mac computers with an SMSID configured.
7. In the **Edit Discovery Script** dialog box, enter the following Shell Script:

```
defaults read com.microsoft.ccmclient SMSID
```

8. Choose **OK** to close the **Edit Discovery Script** dialog box.
9. In the **Create Setting** dialog box, for **Remediation script (optional)**, choose **Add script** to specify a script that removes the SMSID when it is found on Mac computers.
10. In the **Create Remediation Script** dialog box, enter the following Shell Script:

```
defaults delete com.microsoft.ccmclient SMSID
```

11. Choose **OK** to close the **Create Remediation Script** dialog box.
12. On the **Compliance Rules** page of the wizard, click **New**, and then in the **Create Rule** dialog box, specify the following information:
    - **Name:Remove SMSID for Mac**
    - **Selected setting:** Choose **Browse** and then select the discovery script that you specified previously.
    - In **the following values** field, enter **The domain/default pair of (com.microsoft.ccmclient, SMSID) does not exist**.
    - Enable the option **Run the specified remediation script when this setting is noncompliant**.
13. Complete the Create Configuration Item Wizard.
14. Create a configuration baseline that contains the configuration item that you have just created and deploy it to the device collection that you created in step 1.

    For more information about how to create and deploy configuration baselines, see How to create configuration baselines in System Center Configuration Manager and How to deploy configuration baselines in System Center Configuration Manager.
15. On Mac computers that have the SMSID removed, run the following command to install a new certificate:

```
sudo ./CMEnroll -s <enrollment_proxy_server_name> -ignorecertchainvalidation -u <'user name'>
```

    When prompted, provide the password for the super user account to run the command and then the password for the Active Directory user account.
16. To limit the enrolled certificate to Configuration Manager, on the Mac computer, open a terminal window and make the following changes:

    a. Enter the command `sudo /Applications/Utilities/Keychain\ Access.app/Contents/MacOS/Keychain\ Access`

    b. In the **Keychain Access** dialog, in the **Keychains** section, choose **System**, and then, in the **Category** section, choose **Keys**.

    c. Expand the keys to view the client certificates. When you have identified the certificate with a private key that you have just installed, double-click the key.

d. On the **Access Control** tab, choose **Confirm before allowing access**.

e. Browse to **/Library/Application Support/Microsoft/CCM**, select **CCMClient**, and then choose **Add**.

f. Choose **Save Changes** and close the **Keychain Access** dialog box.

17. Restart the Mac computer.

Surface device dashboard in System Center Configuration Manager

7/19/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

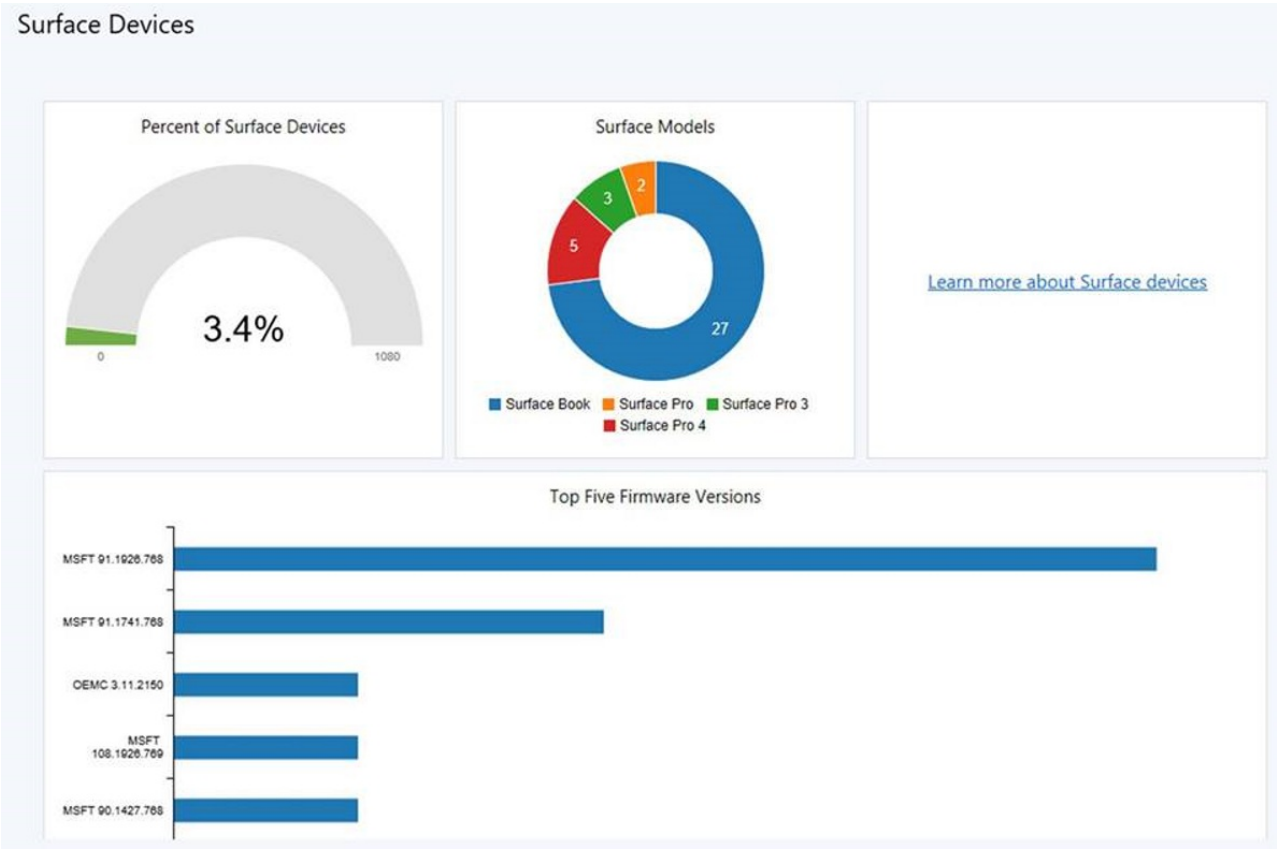
Beginning in version 1802, the Surface device dashboard gives you information about Surface devices found in your environment at a single glance.

Open the Surface device dashboard

To open the Surface device dashboard, use the following steps:

1. Open the Configuration Manager console.
2. Click on the **Monitoring** node.
3. To load the dashboard, click on **Surface Devices**.

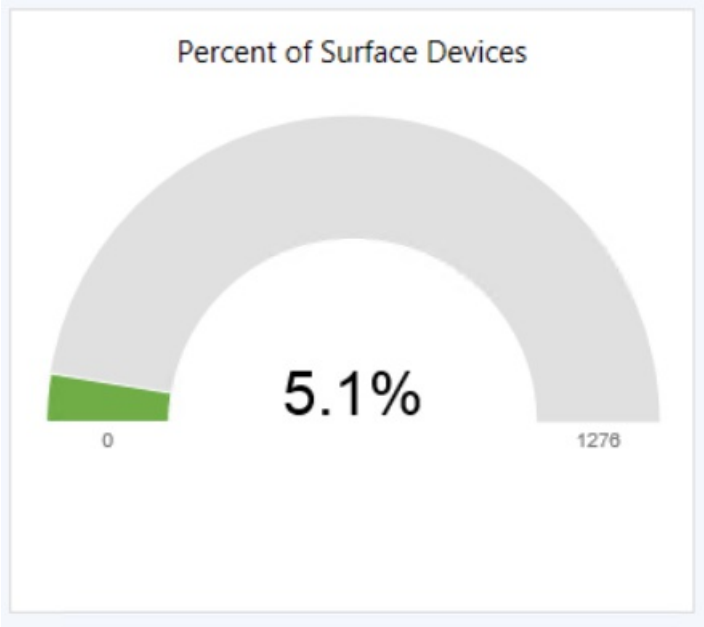
Surface device dashboard



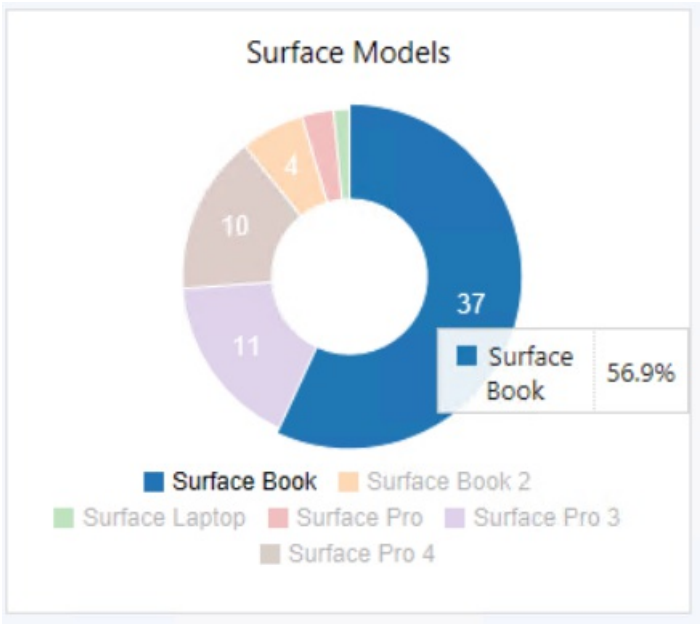
Reviewing information in the Surface device dashboard

The Surface device dashboard shows three graphs for your environment.

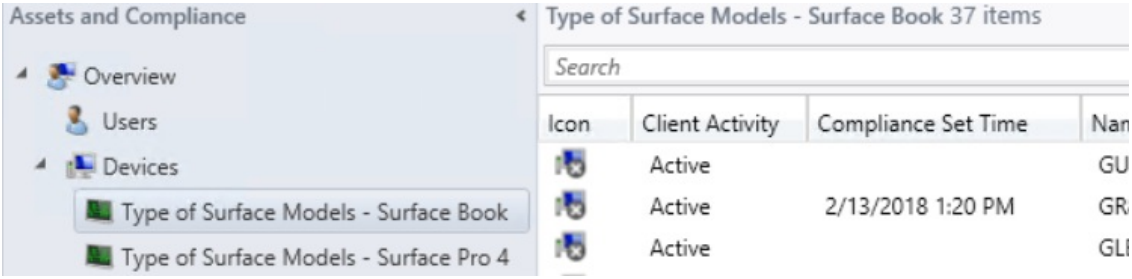
- **Percent of Surface devices** -Gives you the percentage of Surface devices throughout your environment.



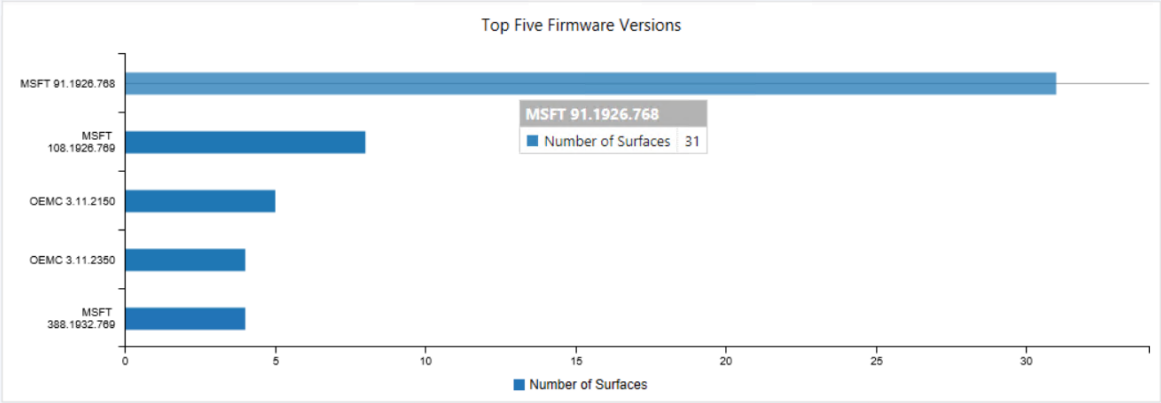
- **Surface Models** -Shows the number of devices per Surface model.
  - Hovering over a graph section will give you the percentage of Surface devices that are the model selected.



  - Clicking on a graph section will take you to a device list for the model.



- **Top five firmware versions**- Displays a chart with the top five firmware models in your environment.
  - Hovering over a graph section will give you the number of Surface devices that are the firmware version selected. Starting in Configuration Manager version 1806, clicking on a graph section displays a list of relevant devices.



More information

For more information about Surface devices, see:

- The Surface website.

For more information about deploying Surface firmware updates in Configuration Manager, see:

- How to manage Surface driver updates in Configuration Manager.

Manage clients on the internet with Configuration Manager

7/26/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Typically in Configuration Manager, most of the managed computers and servers are physically on the same internal network as the site system servers that perform management functions. However, you can manage clients outside your internal network when they are connected to the internet. This ability doesn't require the clients to connect via VPN to reach the site system servers.

Configuration Manager provides two ways to manage internet-connected clients:

- Cloud management gateway
- Internet-based client management

Cloud management gateway

The cloud management gateway provides management of internet-based clients. It uses a combination of a Microsoft Azure cloud service, and a new site system role that communicates with that service. Internet-based clients use the cloud service to communicate with the on-premises Configuration Manager.

Advantages

- No additional on-premises infrastructure investment required.
- Does not expose on-premises infrastructure to the internet.
- Cloud virtual machines that run the service are fully managed by Azure and require no maintenance.
- Easily set up and configured in the Configuration Manager console.

Disadvantages

- Cloud subscription cost.
- Management data sent through cloud service.

For more information, see Plan for cloud management gateway.

Internet-based client management

This method relies on internet-facing site system servers to which clients communicate for management purposes. It requires clients and site system servers to be configured for internet-based management.

Advantages

- No cloud service dependency.
- No additional cost associated with a cloud subscription.
- Full control of servers and roles providing the service.

Disadvantages

- Require additional infrastructure investment.
- Overhead and operational cost of additional infrastructure.

- Infrastructure must be exposed to the internet.

For more information, see Plan for internet-based client management.

Plan for the cloud management gateway in Configuration Manager

8/6/2019 • 17 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The cloud management gateway (CMG) provides a simple way to manage Configuration Manager clients on the internet. By deploying the CMG as a cloud service in Microsoft Azure, you can manage traditional clients that roam on the internet without additional on-premises infrastructure. You also don't need to expose your on-premises infrastructure to the internet.

> **NOTE**
> Configuration Manager doesn't enable this optional feature by default. You must enable this feature before using it. For more information, see Enable optional features from updates.

After establishing the prerequisites, creating the CMG consists of the following three steps in the Configuration Manager console:

1. Deploy the CMG cloud service to Azure.
2. Add the CMG connection point role.
3. Configure the site and site roles for the service. Once deployed and configured, clients seamlessly access on-premises site roles regardless of whether they're on the intranet or internet.

This article provides the foundational knowledge to learn about the CMG, design how it fits in your environment, and plan the implementation.

Scenarios

There are several scenarios for which a CMG is beneficial. The following scenarios are some of the more common:

- Manage traditional Windows clients with Active Directory domain-joined identity. These clients include Windows 7, Windows 8.1, and Windows 10. It uses PKI certificates to secure the communication channel. Management activities include:
  - Software updates and endpoint protection
  - Inventory and client status
  - Compliance settings
  - Software distribution to the device
  - Windows 10 in-place upgrade task sequence
- Manage traditional Windows 10 clients with modern identity, either hybrid or pure cloud domain-joined with Azure Active Directory (Azure AD). Clients use Azure AD to authenticate rather than PKI certificates. Using Azure AD is simpler to set up, configure and maintain than more complex PKI systems. Management activities are the same as the first scenario, as well as:
  - Software distribution to the user
- Install the Configuration Manager client on Windows 10 devices over the internet. Using Azure AD allows the device to authenticate to the CMG for client registration and assignment. You can install the client manually, or using another software distribution method, such as Microsoft Intune.

- New device provisioning with co-management. When auto-enrolling existing clients, CMG isn't required for co-management. It is required for new devices involving Windows AutoPilot, Azure AD, Microsoft Intune, and Configuration Manager. For more information, see Paths to co-management.

Specific use cases

Across these scenarios the following specific device use cases may apply:

- Roaming devices such as laptops
- Remote/branch office devices that are less expensive and more efficient to manage over the internet than across a WAN or through a VPN.
- Mergers and acquisitions, where it may be easiest to join devices to Azure AD and manage through a CMG.

> **IMPORTANT**
> By default all clients receive policy for a CMG, and start using it when they become internet-based. Depending upon the scenario and use case that applies to your organization, you may need to scope usage of the CMG. For more information, see the Enable clients to use a cloud management gateway client setting.

Topology design

CMG components

Deployment and operation of the CMG includes the following components:

- The **CMG cloud service** in Azure authenticates and forwards Configuration Manager client requests to the CMG connection point.
- The **CMG connection point** site system role enables a consistent and high-performance connection from the on-premises network to the CMG service in Azure. It also publishes settings to the CMG including connection information and security settings. The CMG connection point forwards client requests from the CMG to on-premises roles according to URL mappings.
- The **service connection point** site system role runs the cloud service manager component, which handles all CMG deployment tasks. Additionally, it monitors and reports service health and logging information from Azure AD. Make sure your service connection point is in online mode.
- The **management point** site system role services client requests per normal.
- The **software update point** site system role services client requests per normal.
- **Internet-based clients** connect to the CMG to access on-premises Configuration Manager components.
- The CMG uses a **certificate-based HTTPS** web service to help secure network communication with clients.
- Internet-based clients use **PKI certificates or Azure AD** for identity and authentication.
- A **cloud distribution point** provides content to internet-based clients, as needed.
    - Starting in version 1806, a CMG can also serve content to clients. This functionality reduces the required certificates and cost of Azure VMs. For more information, see Modify a CMG.

Azure Resource Manager

Create the CMG using an **Azure Resource Manager deployment**. Azure Resource Manager is a modern platform for managing all solution resources as a single entity, called a resource group. When deploying CMG with Azure Resource Manager, the site uses Azure Active Directory (Azure AD) to authenticate and create the necessary cloud resources. This modernized deployment doesn't require the classic Azure management certificate.

> **NOTE**
>
> This capability doesn't enable support for Azure Cloud Service Providers (CSP). The CMG deployment with Azure Resource Manager continues to use the classic cloud service, which the CSP doesn't support. For more information, see available Azure services in Azure CSP.

Starting in Configuration Manager version 1902, Azure Resource Manager is the only deployment mechanism for new instances of the cloud management gateway. Existing deployments continue to work.

In Configuration Manager version 1810 and earlier, the CMG wizard still provides the option for a **classic service deployment** using an Azure management certificate. To simplify the deployment and management of resources, the Azure Resource Manager deployment model is recommended for all new CMG instances. If possible, redeploy existing CMG instances through Resource Manager. For more information, see Modify a CMG.

> **IMPORTANT**
>
> Starting in version 1810, the classic service deployment in Azure is deprecated for use in Configuration Manager. This version is the last to support creation of these Azure deployments. This functionality will be removed in a future Configuration Manager version.

Hierarchy design

Create the CMG at the top-tier site of your hierarchy. If that's a central administration site, then create CMG connection points at child primary sites. The cloud service manager component is on the service connection point, which is also on the central administration site. This design can share the service across different primary sites if needed.

You can create multiple CMG services in Azure, and you can create multiple CMG connection points. Multiple CMG connection points provide load balancing of client traffic from the CMG to the on-premises roles. To reduce network latency, assign the associated CMG to the same geographical region as the primary site.

Starting in version 1902, you can associate a CMG with a boundary group. This configuration allows clients to default or fallback to the CMG for client communication according to boundary group relationships. This behavior is especially useful in branch office and VPN scenarios. You can direct client traffic away from expensive and slow WAN links to instead use faster services in Microsoft Azure.

> **NOTE**
>
> Internet-based clients don't fall into any boundary group.
>
> In Configuration Manager version 1810 and earlier, the CMG doesn't fall into any boundary group.

Other factors, such as the number of clients to manage, also impact your CMG design. For more information, see Performance and scale.

Example 1: standalone primary site

Contoso has a standalone primary site in an on-premises datacenter at their headquarters in New York City.

- They create a CMG in the East US Azure region to reduce network latency.
- They create two CMG connection points, both linked to the single CMG service.

As clients roam onto the internet, they communicate with the CMG in the East US Azure region. The CMG forwards this communication through both of the CMG connection points.

Example 2: hierarchy with site-specific CMG

Fourth Coffee has a central administration site in an on-premises datacenter at their headquarters in Seattle. One

primary site is in the same datacenter, and the other primary site is in their main European office in Paris.

- On the central administration site, they create two CMG services:
  - One CMG in the West US Azure region.
  - One CMG in the West Europe Azure region.
- On the Seattle-based primary site, they create a CMG connection point linked to the West US CMG.
- On the Paris-based primary site, they create a CMG connection point linked to the West Europe CMG.

As Seattle-based clients roam onto the internet, they communicate with the CMG in the West US Azure region. The CMG forwards this communication to the Seattle-based CMG connection point.

Similarly, as Paris-based clients roam onto the internet, they communicate with the CMG in the West Europe Azure region. The CMG forwards this communication to the Paris-based CMG connection point. When Paris-based users travel to the company headquarters in Seattle, their computers continue to communicate with the CMG in the West Europe Azure region.

> **NOTE**
> Fourth Coffee considered creating another CMG connection point on the Paris-based primary site linked to the West US CMG. Paris-based clients would then use both CMGs, regardless of their location. While this configuration helps load balance traffic and provide service redundancy, it can also cause delays when Paris-based clients communicate with the US-based CMG. Configuration Manager clients aren't currently aware of their geographical region, so don't prefer a CMG that's geographically closer. Clients randomly use an available CMG.

Requirements

- An **Azure subscription** to host the CMG.
- An **Azure administrator** needs to participate in the initial creation of certain components, depending upon your design. This persona doesn't require permissions in Configuration Manager.
  - To deploy the CMG, you need a **Subscription Admin**
  - To integrate the site with Azure AD for deploying the CMG using Azure Resource Manager, you need a **Global Admin**
- At least one on-premises Windows server to host the **CMG connection point**. You can colocate this role with other Configuration Manager site system roles.
- The **service connection point** must be in online mode.
- Integration with **Azure AD** for deploying the service with Azure Resource Manager. For more information, see Configure Azure services.
- A **server authentication certificate** for the CMG.
- **Other certificates** may be required, depending upon your client OS version and authentication model. For more information, see CMG certificates.

  Starting in version 1806, when using the site option to **Use Configuration Manager-generated certificates for HTTP site systems**, the management point can be HTTP. For more information, see Enhanced HTTP.
- In Configuration Manager version 1810 or earlier, if using the Azure classic deployment method, you must use an **Azure management certificate**.

> **TIP**
>
> Use the **Azure Resource Manager** deployment model. It doesn't require this management certificate.
>
> The classic deployment method is deprecated as of version 1810.

- Clients must use **IPv4**.

Specifications

- All Windows versions listed in Supported operating systems for clients and devices are supported for CMG.
- CMG only supports the management point and software update point roles.
- CMG doesn't support clients that only communicate with IPv6 addresses.
- Software update points using a network load balancer don't work with CMG.
- CMG deployments using the Azure Resource Model don't enable support for Azure Cloud Service Providers (CSP). The CMG deployment with Azure Resource Manager continues to use the classic cloud service, which the CSP doesn't support. For more information, see available Azure services in Azure CSP

Support for Configuration Manager features

The following table lists CMG support for Configuration Manager features:

FEATURE	SUPPORT
Software updates	✓
Endpoint protection	✓
Hardware and software inventory	✓
Client status and notifications	✓
Run scripts	✓
Compliance settings	✓
Client install (with Azure AD integration)	✓
Software distribution (device-targeted)	✓
Software distribution (user-targeted, required) (with Azure AD integration)	✓
Software distribution (user-targeted, available) (all requirements)	✓
Windows 10 in-place upgrade task sequence	✓

FEATURE	SUPPORT
Task sequences that aren't using boot images and are deployed with an option: **Download all content locally before starting task sequence**	✅
CMPivot	✅ (1806)
Any other task sequence scenario	❌
Client push	❌
Automatic site assignment	❌
Software approval requests	❌
Configuration Manager console	❌
Remote tools	❌
Reporting website	❌
Wake on LAN	❌
Mac, Linux, and UNIX clients	❌
Peer cache	❌
On-premises MDM	❌

KEY
✅ = This feature is supported with CMG by all supported versions of Configuration Manager
✅ (*YYMM*) = This feature is supported with CMG starting with version *YYMM* of Configuration Manager
❌ = This feature isn't supported with CMG

Cost

> **IMPORTANT**
> The following cost information is for estimating purposes only. Your environment may have other variables that affect the overall cost of using CMG.

CMG uses the following Azure components, which incur charges to the Azure subscription account:

Virtual machine

- CMG uses Azure Cloud Services as platform as a service (PaaS). This service uses virtual machines (VMs)

that incur compute costs.

- CMG uses a Standard A2 V2 VM.
- You select how many VM instances support the CMG. One is the default, and 16 is the maximum. This number is set when creating the CMG, and can be changed afterwards to scale the service as needed.
- For more information on how many VMs you need to support your clients, see Performance and scale.
- See the Azure pricing calculator to help determine potential costs.

> **NOTE**
> Virtual machine costs vary by region.

Outbound data transfer

- Charges are based on data flowing out of Azure (egress or download). Any data flows into Azure are free (ingress or upload). CMG data flows out of Azure include policy to the client, client notifications, and client responses forwarded by the CMG to the site. These responses include inventory reports, status messages, and compliance status.
- Even without any clients communicating with a CMG, some background communication causes network traffic between the CMG and the on-premises site.
- View the **Outbound data transfer (GB)** in the Configuration Manager console. For more information, see Monitor clients on CMG.
- See the Azure bandwidth pricing details to help determine potential costs. Pricing for data transfer is tiered. The more you use, the less you pay per gigabyte.
- *For estimating purposes only*, expect approximately 100-300 MB per client per month for internet-based clients. The lower estimate is for a default client configuration. The upper estimate is for a more aggressive client configuration. Your actual usage may vary depending upon how you configure client settings.

> **NOTE**
> Performing other actions, such as deploying software updates or applications, increases the amount of outbound data transfer from Azure.

- Misconfiguration of the CMG option to **Verify client certificate revocation** can cause additional traffic from clients to the CMG. This additional traffic can increase the Azure egress data, which can increase your Azure costs. For more information, see Publish the certificate revocation list.

Content storage

- Internet-based clients get Microsoft software update content from Windows Update at no charge. Don't distribute update packages with Microsoft update content to a cloud distribution point, otherwise you may incur storage and data egress costs.
- For any other necessary content, such as applications or third-party software updates, you must distribute to a cloud distribution point. Currently, the CMG supports only the cloud distribution point for sending content to clients.
- For more information, see the cost of using cloud distribution points.
- Starting in version 1806, a CMG can also be a cloud distribution point to serve content to clients. This functionality reduces the required certificates and cost of Azure VMs. For more information, see Modify a CMG.

Other costs

- Each cloud service has a dynamic IP address. Each distinct CMG uses a new dynamic IP address. Adding additional VMs per CMG doesn't increase these addresses.

Performance and scale

For more information on CMG scale, see Size and scale numbers.

The following recommendations can help you improve CMG performance:

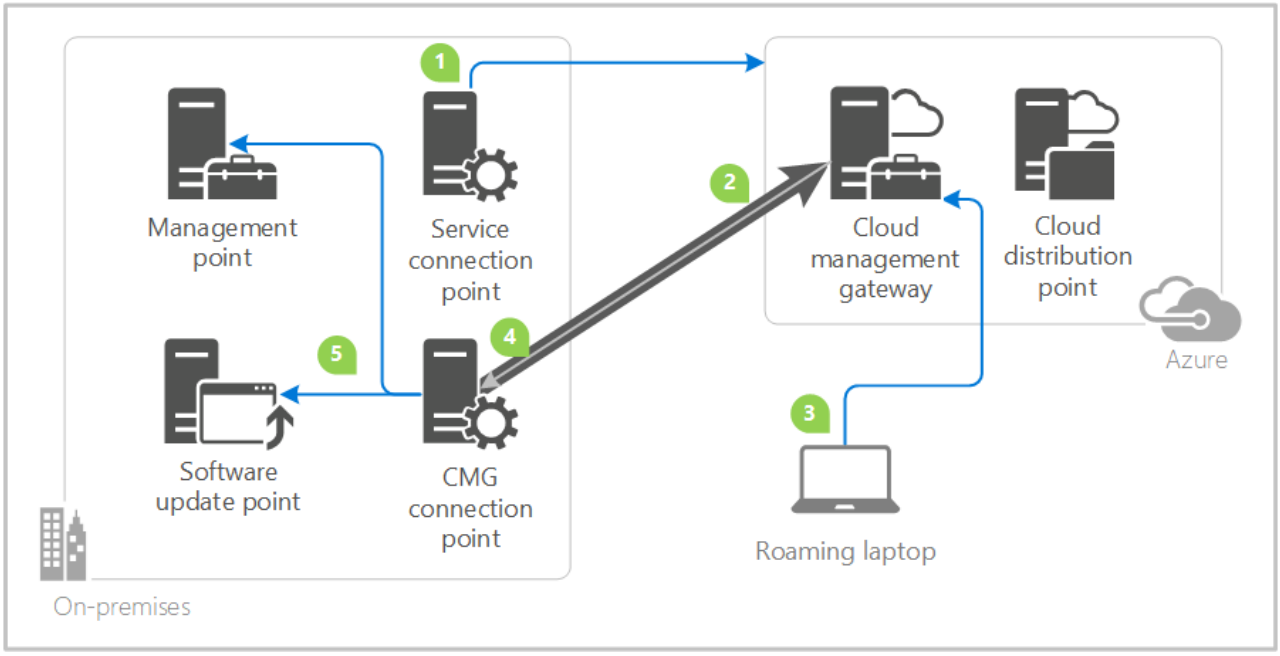
- If possible, configure the CMG, CMG connection point, and the Configuration Manager site server in same network region to reduce latency.
- The connection between the Configuration Manager client and the CMG isn't region-aware. Client communication is largely unaffected by latency / geographic separation. It's not necessary to deploy multiple CMG for the purposes of geo-proximity. Deploy the CMG at the top-level site in your hierarchy and add instances to increase scale.
- For high availability of the service, create a CMG with at least two CMG instances and two CMG connection points per site.
- Scale the CMG to support more clients by adding more VM instances. The Azure load balancer controls client connections to the service.
- Create more CMG connection points to distribute the load among them. The CMG distributes the traffic to its connecting CMG connection points in a round-robin fashion.
- When the CMG is under high load with more than the supported number of clients, it still handles requests but there may be delay.

> **NOTE**
> While Configuration Manager has no hard limit on the number of clients for a CMG connection point, Windows Server has a default maximum TCP dynamic port range of 16,384. If a Configuration Manager site manages more than 16,384 clients with a single CMG connection point, you must increase the Windows Server limit. All clients maintain a channel for client notifications, which holds a port open on the CMG connection point. For more information on how to use the netsh command to increase this limit, see Microsoft Support article 929851.

Ports and data flow

You don't need to open any inbound ports to your on-premises network. The service connection point and CMG connection point initiate all communication with Azure and the CMG. These two site system roles need to create outbound connections to the Microsoft cloud. The service connection point deploys and monitors the service in Azure, thus must be online mode. The CMG connection point connects to the CMG to manage communication between the CMG and on-premises site system roles.

The following diagram is a basic, conceptual data flow for the CMG:



1. The service connection point connects to Azure over HTTPS port 443. It authenticates using Azure AD or the Azure management certificate. The service connection point deploys the CMG in Azure. The CMG creates the HTTPS cloud service using the server authentication certificate.
2. The CMG connection point connects to the CMG in Azure over TCP-TLS or HTTPS. It holds the connection open, and builds the channel for future two-way communication.
3. The client connects to the CMG over HTTPS port 443. It authenticates using Azure AD or the client authentication certificate.
4. The CMG forwards the client communication over the existing connection to the on-premises CMG connection point. You don't need to open any inbound firewall ports.
5. The CMG connection point forwards the client communication to the on-premises management point and software update point.

For more information when you host content in Azure, see Use a cloud-based distribution point.

Required ports

This table lists the required network ports and protocols. The *Client* is the device initiating the connection, requiring an outbound port. The *Server* is the device accepting the connection, requiring an inbound port.

CLIENT	PROTOCOL	PORT	SERVER	DESCRIPTION
Service connection point	HTTPS	443	Azure	CMG deployment
CMG connection point	TCP-TLS	10140-10155	CMG service	Preferred protocol to build CMG channel [1]
CMG connection point	HTTPS	443	CMG service	Fallback protocol to build CMG channel to only one VM instance[2]
CMG connection point	HTTPS	10124-10139	CMG service	Fallback protocol to build CMG channel to two or more VM instances[3]

CLIENT	PROTOCOL	PORT	SERVER	DESCRIPTION
Client	HTTPS	443	CMG	General client communication
CMG connection point	HTTPS or HTTP	443 or 80	Management point (version 1710)	On-premises traffic, port depends upon management point configuration
CMG connection point	HTTPS	443	Management point (version 1802)	On-premises traffic must be HTTPS
CMG connection point	HTTPS or HTTP	443 or 80	Software update point	On-premises traffic, port depends upon software update point configuration

[1] The CMG connection point first tries to establish a long-lived TCP-TLS connection with each CMG VM instance. It connects to the first VM instance on port 10140. The second VM instance uses port 10141, up to the 16th on port 10155. A TCP-TLS connection performs the best, but it doesn't support internet proxy. If the CMG connection point can't connect via TCP-TLS, then it falls back to HTTPS[2].

[2] If the CMG connection point can't connect to the CMG via TCP-TLS[1], it connects to the Azure network load balancer over HTTPS 443 only for one VM instance.

[3] If there are two or more VM instances, the CMG connection point uses HTTPS 10124 to the first VM instance, not HTTPS 443. It connects to the second VM instance on HTTPS 10125, up to the 16th on HTTPS port 10139.

Internet access requirements

If your organization restricts network communication with the internet using a firewall or proxy device, you need to allow CMG connection point and service connection point to access internet endpoints.

For more information, see Internet access requirements.

Next steps

- Certificates for cloud management gateway
- Security and privacy for cloud management gateway
- Cloud management gateway size and scale numbers
- Frequently asked questions about the cloud management gateway
- Set up cloud management gateway

Security and privacy for the cloud management gateway

7/26/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article includes security and privacy information for the Configuration Manager cloud management gateway (CMG). For more information, see Plan for cloud management gateway.

CMG security details

- The CMG accepts and manages connections from CMG connection points. It uses mutual SSL authentication using certificates and connection IDs.
- The CMG accepts and forwards client requests using the following methods:
  - Pre-authenticates connections using mutual SSL with the PKI-based client authentication certificate or Azure AD.
    - IIS on the CMG VM instances verifies the certificate path based on the trusted root certificate(s) uploaded to the CMG.
    - IIS on the VM instance also verifies client certificate revocation, if enabled. For more information, see Publish the certificate revocation list.
  - The certificate trust list checks the root of the client authentication certificate. It also performs the same validation as the management point for the client. For more information, see Review entries in the site's certificate trust list.
  - Validates and filters client requests (URLs) to check if any CMG connection point can service the request.
  - Checks content length for each publishing endpoint.
  - Uses round-robin behavior to load-balance CMG connection points in the same site.
- The CMG connection point uses the following methods:
  - Builds consistent HTTPS/TCP connections to all VM instances of the CMG. It checks and maintains these connections every minute.
  - Uses mutual SSL authentication with the CMG using certificates.
  - Forwards client requests based on URL mappings.
  - Reports connection status to show service health status in the console.
  - Reports traffic per endpoint every five minutes.

Configuration Manager client-facing roles

The management point and software update point host endpoints in IIS to service client requests. The CMG doesn't expose all internal endpoints. Every endpoint published to the CMG has an URL mapping.

- The external URL is the one the client uses to communicate with the CMG.
- The internal URL is the CMG connection point used to forward requests to the internal server.

URL mapping example

When you enable CMG traffic on a management point, Configuration Manager creates an internal set of URL mappings for each management point server. For example: ccm_system, ccm_incoming, and sms_mp. The external URL for the management point ccm_system endpoint might look like:

```
https://<CMG service name>/CCM_Proxy_MutualAuth/<MP Role ID>/CCM_System
```

The URL is unique for each management point. The Configuration Manager client then puts the CMG-enabled management point name into its internet management point list. This name looks like:

`<CMG service name>/CCM_Proxy_MutualAuth/<MP Role ID>`

The site automatically uploads all published external URLs to the CMG. This behavior allows the CMG to do URL filtering. All URL mappings replicate to the CMG connection point. It then forwards the communication to internal servers according to the external URL from the client request.

Security guidance for CMG

Publish the certificate revocation list

Publish your PKI's certificate revocation list (CRL) for internet-based clients to access. When deploying a CMG using PKI, configure the service to **verify client certificate revocation** on the Settings tab. This setting configures the service to use a published certificate revocation list (CRL). For more information, see Plan for PKI certificate revocation.

This CMG option verifies the client authentication certificate.

- If the client is using Azure AD authentication, the CRL doesn't matter.
- If you use PKI, and externally publish the CRL, then enable this option (recommended).
- If you use PKI, don't publish the CRL, then disable this option.
- If you misconfigure this option, it can cause additional traffic from clients to the CMG. This additional traffic can increase the Azure egress data, which can increase your Azure costs.

Review entries in the site's certificate trust list

Each Configuration Manager site includes a list of trusted root certification authorities, the certificate trust list (CTL). View and modify the list by going to the Administration workspace, expand Site Configuration, and select Sites. Select a site, and click Properties in the ribbon. Switch to the **Client Computer Communication** tab, and then click **Set** under Trusted Root Certification Authorities.

> **NOTE**
> Starting in version 1906, this tab is called **Communication Security**.

Use a more restrictive CTL for a site with a CMG using PKI client authentication. Otherwise, clients with client authentication certificates issued by any trusted root that already exists on the management point are automatically accepted for client registration.

This subset provides administrators with more control over security. The CTL restricts the server to only accept client certificates that are issued from the certification authorities in the CTL. For example, Windows ships with a number of well-known third-party certification authority (CA) certificates, such as VeriSign and Thawte. By default, the computer running IIS trusts certificates that chain to these well-known CAs. Without configuring IIS with a CTL, any computer that has a client certificate issued from these CAs are accepted as a valid Configuration Manager client. If you configure IIS with a CTL that didn't include these CAs, client connections are refused if the certificate chained to these CAs.

Enforce TLS 1.2

Starting in version 1906, use the CMG setting to **Enforce TLS 1.2**. It only applies to the Azure cloud service VM. It doesn't apply to any on-premises Configuration Manager site servers or clients. For more information on TLS 1.2, see How to enable TLS 1.2.

Next steps

- Plan for cloud management gateway
- Set up cloud management gateway
- Frequently asked questions about the cloud management gateway

- Certificates for cloud management gateway

Frequently asked questions about the cloud management gateway

7/15/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article answers your frequently asked questions about the cloud management gateway. For more information, see plan for cloud management gateway.

Frequently asked questions

What certificates do I need?

For more detailed information, see certificates for cloud management gateway.

Do I need Azure ExpressRoute?

No. Azure ExpressRoute lets you extend your on-premises network into the Microsoft cloud. ExpressRoute, or other such virtual network connections aren't required for the Configuration Manager cloud management gateway. The design of the cloud management gateway allows internet-based clients to communicate through the Azure service to on-premises site systems with no additional network configuration. For more information, see Plan for cloud management gateway

Do I need to maintain the Azure virtual machines?

No maintenance is required. The design of the cloud management gateway uses Azure platform as a service (PaaS). Using the subscription you provide, Configuration Manager creates the necessary virtual machines (VMs), storage, and networking. Azure secures and updates the virtual machine. These VMs aren't a part of your on-premises environment, as is the case with infrastructure as a service (IaaS). The cloud management gateway is a PaaS that extends your Configuration Manager environment into the cloud. For more information, see Securing PaaS deployments.

How can I ensure service continuity during service updates?

By scaling CMG to include two or more instances, you automatically benefit from Update Domains in Azure. See How to update a cloud service.

I'm already using IBCM. If I add CMG, how do clients behave?

If you already deployed internet-based client management (IBCM), you can also deploy the cloud management gateway. Clients receive policy for both services. As they roam onto the internet, they randomly select and use one of these internet-based services.

Do the user accounts have to be in the same Azure subscription as the subscription that hosts the CMG cloud service?

If your environment has more than one subscription, you can deploy CMG into any subscription that can host Azure cloud services.

This question is common in the following scenarios:

- When you have distinct test and production Active Directory and Azure AD environments, but one single, centralized Azure hosting subscription
- Your use of Azure has grown organically across different teams

When you're using a Resource Manager deployment, onboard the associated Azure AD tenant. This connection

allows Configuration Manager to authenticate to Azure to create, deploy, and manage the CMG.

If you're using Azure AD authentication for the users and devices managed over the CMG, onboard that Azure AD tenant. For more information on Azure services for cloud management, see Configure Azure services. When you onboard each Azure AD tenant, a single CMG can provide Azure AD authentication for multiple tenants, regardless of the hosting location.

How does CMG affect my clients connected via VPN?

Roaming clients that connect to your environment via a VPN are commonly detected as intranet-facing. They attempt to connect to your on-premises infrastructure such as management points and distribution points. Some customers prefer to have these roaming clients managed by cloud services even when connected via VPN. Starting in version 1902, associate the CMG with a boundary group. This action forces these clients to not use the on-premises site systems. For more information, see Configure boundary groups.

If I enable a CMG, will my clients only connect to the CMG-enabled management point when they're connected to the intranet?

In order to secure sensitive traffic sent over a CMG, either configure an HTTPS management point or use Enhanced HTTP.

If you choose to deploy a CMG, and use PKI certificates for HTTPS communication on the CMG-enabled management point, select the option to **Allow internet-only clients** on the management point properties. This setting makes sure that internal clients continue to use HTTP management points in your environment.

If you use Enhanced HTTP, you don't need to configure this setting. Clients continue to use HTTP when communicating directly to the CMG-enabled management point. For more information, see Enhanced HTTP.

Next steps

- Plan for cloud management gateway
- Set up cloud management gateway
- Certificates for cloud management gateway
- Security and privacy for cloud management gateway
- Cloud management gateway size and scale numbers

Certificates for the cloud management gateway

7/26/2019 • 12 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Depending upon the scenario you use to manage clients on the internet with the cloud management gateway (CMG), you need one or more of the following digital certificates:

- CMG server authentication certificate
  - CMG trusted root certificate to clients
  - Server authentication certificate issued by public provider
  - Server authentication certificate issued from enterprise PKI
- Client authentication certificate
  - Client trusted root certificate to CMG
- Enable management point for HTTPS
- Azure management certificate

For more information about the different scenarios, see plan for cloud management gateway.

General information

Certificates for the cloud management gateway support the following configurations:

- 2048-bit or 4096-bit key length
- Key storage providers for certificate private keys. For more information, see CNG certificates overview.
- When you configure Windows with the following policy: **System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing**
- **TLS 1.2**. For more information, see How to enable TLS 1.2.

CMG server authentication certificate

This certificate is required in all scenarios.

You supply this certificate when creating the CMG in the Configuration Manager console.

The CMG creates an HTTPS service to which internet-based clients connect. The server requires a server authentication certificate to build the secure channel. Acquire a certificate for this purpose from a public provider, or issue it from your public key infrastructure (PKI). For more information, see CMG trusted root certificate to clients.

> **NOTE**
>
> The CMG server authentication certificate supports wildcards. Some certificate authorities issue certificates using a wildcard character for the hostname. For example, `*.contoso.com`. Some organizations use wildcard certificates to simplify their PKI and reduce maintenance costs.
>
> For more information on how to use a wildcard certificate with a CMG, see Set up a CMG.

This certificate requires a globally unique name to identify the service in Azure. Before requesting a certificate, confirm that the Azure domain name you want is unique. For example, *GraniteFalls.CloudApp.Net*.

1. Sign in to the Azure portal.
2. Select **All resources**, and then select **Add**.
3. Search for **Cloud service**. Select **Create**.
4. In the **DNS name** field, type the prefix you want, for example *GraniteFalls*. The interface reflects whether the domain name is available or already in use by another service.

   > **IMPORTANT**
   > Don't create the service in the portal, just use this process to check the name availability.

If you will also enable the CMG for content, confirm that the CMG service name is also a unique Azure storage account name. If the CMG cloud service name is unique, but the storage account name isn't, Configuration Manager fails to provision the service in Azure. Repeat the above process in the Azure portal with the following changes:

- Search for **Storage account**
- Test your name in the **Storage account name** field

The DNS name prefix, for example *GraniteFalls*, should be 3 to 24 characters long, and only use alphanumeric characters. Don't use special characters, like a dash (`-`).

CMG trusted root certificate to clients

Clients must trust the CMG server authentication certificate. There are two methods to accomplish this trust:

- Use a certificate from a public and globally trusted certificate provider. For example, but not limited to, DigiCert, Thawte, or VeriSign. Windows clients include trusted root certificate authorities (CAs) from these providers. By using a server authentication certificate issued by one of these providers, your clients automatically trust it.
- Use a certificate issued by an enterprise CA from your public key infrastructure (PKI). Most enterprise PKI implementations add the trusted root CAs to Windows clients. For example, using Active Directory Certificate Services with group policy. If you issue the CMG server authentication certificate from a CA that your clients don't automatically trust, add the CA trusted root certificate to internet-based clients.
  - You can also use Configuration Manager certificate profiles to provision certificates on clients. For more information, see Introduction to certificate profiles.
  - If you plan to install the Configuration Manager client from Intune, you can also use Intune certificate profiles to provision certificates on clients. For more see Configure a certificate profile.

Server authentication certificate issued by public provider

A third-party certificate provider can't create a certificate for CloudApp.net, as that domain is owned by Microsoft. You can only get a certificate issued for a domain you own. The main reason for acquiring a certificate from a third-party provider is that your clients already trust that provider's root certificate.

Use the following process to create a DNS alias:

1. Create a canonical name record (CNAME) in your organization's public DNS. This record creates an alias for the CMG to a friendly name that you use in the public certificate.

   For example, Contoso names their CMG **GraniteFalls**. This name becomes **GraniteFalls.CloudApp.Net** in Azure. In Contoso's public DNS contoso.com namespace, the DNS administrator creates a new CNAME

record for **GraniteFalls.Contoso.com** for the real host name, **GraniteFalls.CloudApp.net**.

2. Request a server authentication certificate from a public provider using the Common Name (CN) of the CNAME alias. For example, Contoso uses **GraniteFalls.Contoso.com** for the certificate CN.

3. Create the CMG in the Configuration Manager console using this certificate. On the **Settings** page of the Create Cloud Management Gateway Wizard:

   - When you add the server certificate for this cloud service (from **Certificate file**), the wizard extracts the hostname from the certificate CN as the service name.

   - It then appends that hostname to **cloudapp.net**, or **usgovcloudapp.net** for the Azure US Government cloud, as the Service FQDN to create the service in Azure.

   - For example, when Contoso creates the CMG, Configuration Manager extracts the hostname **GraniteFalls** from the certificate CN. Azure creates the actual service as **GraniteFalls.CloudApp.net**.

When you create the CMG instance in Configuration Manager, while the certificate has GraniteFalls.Contoso.com, Configuration Manager only extracts the hostname, for example: GraniteFalls. It appends this hostname to CloudApp.net, which Azure requires when creating a cloud service. The CNAME alias in the DNS namespace for your domain, Contoso.com, maps together these two FQDNs. Configuration Manager gives clients a policy to access this CMG, the DNS mapping ties it together so that they can securely access the service in Azure.

Server authentication certificate issued from enterprise PKI

Create a custom SSL certificate for the CMG the same as for a cloud distribution point. Follow the instructions for Deploying the service certificate for cloud-based distribution points but do the following things differently:

- When requesting the custom web server certificate, provide an FQDN for the certificate's common name. This name can be a public domain name you own or you may use the cloudapp.net domain. If using your own public domain, refer to the process above for creating a DNS alias in your organization's public DNS.

- When using the cloudapp.net public domain for the CMG web server certificate:

  - On the Azure public cloud, use a name that ends in **cloudapp.net**

  - Use a name that ends in **usgovcloudapp.net** for the Azure US Government cloud

Client authentication certificate

This certificate is required for internet-based clients running Windows 7, Windows 8.1, and Windows 10 devices not joined to Azure Active Directory (Azure AD). It's also required on the CMG connection point. It isn't required for Windows 10 clients joined to Azure AD.

The clients use this certificate to authenticate with the CMG. Windows 10 devices that are hybrid or cloud domain-joined don't require this certificate because they use Azure AD to authenticate.

Provision this certificate outside of the context of Configuration Manager. For example, use Active Directory Certificate Services and group policy to issue client authentication certificates. For more information, see Deploying the client certificate for Windows computers.

To securely forward client requests, the CMG connection point requires a client authentication certificate that corresponds to the server authentication certificate on the HTTPS management point. If clients use Azure AD authentication, or you configure the management point for Enhanced HTTP, this certificate isn't required. For more information, see Enable management point for HTTPS.

Client trusted root certificate to CMG

This certificate is required when using client authentication certificates. When all clients use Azure AD for

authentication, this certificate isn't required.

You supply this certificate when creating the CMG in the Configuration Manager console.

The CMG must trust the client authentication certificates. To accomplish this trust, provide the trusted root certificate chain. Make sure to add all certificates in the trust chain. For example, if the client authentication certificate is issued by an intermediate CA, add both the intermediate and root CA certificates.

> **NOTE**
>
> Starting in version 1806, when you create a CMG, you're no longer required to provide a trusted root certificate on the Settings page. This certificate isn't required when using Azure Active Directory (Azure AD) for client authentication, but used to be required in the wizard. If you're using PKI client authentication certificates, then you still must add a trusted root certificate to the CMG.
>
> In version 1902 and earlier, you can only add two trusted root CAs and four intermediate (subordinate) CAs.

Export the client certificate's trusted root

After issuing a client authentication certificate to a computer, use this process on that computer to export the trusted root.

1. Open the Start menu. Type "run" to open the Run window. Open `mmc`.
2. From the File menu, choose **Add/Remove Snap-in...**.
3. In the Add or Remove Snap-ins dialog box, select **Certificates**, then select **Add**.
   a. In the Certificates snap-in dialog box, select **Computer account**, then select **Next**.
   b. In the Select Computer dialog box, select **Local computer**, then select **Finish**.
   c. In the Add or Remove Snap-ins dialog box, select **OK**.
4. Expand **Certificates**, expand **Personal**, and select **Certificates**.
5. Select a certificate whose Intended Purpose is **Client Authentication**.
   a. From the Action menu, select **Open**.
   b. Go to the **Certification Path** tab.
   c. Select the next certificate up the chain, and select **View Certificate**.
6. On this new Certificate dialog box, go to the **Details** tab. Select **Copy to File...**.
7. Complete the Certificate Export Wizard using the default certificate format, **DER encoded binary X.509 (.CER)**. Make note of the name and location of the exported certificate.
8. Export all of the certificates in the certification path of the original client authentication certificate. Make note of which exported certificates are intermediate CAs, and which ones are trusted root CAs.

Enable management point for HTTPS

Provision this certificate outside of the context of Configuration Manager. For example, use Active Directory Certificate Services and group policy to issue a web server certificate. For more information, see PKI certificate requirements and Deploy the web server certificate for site systems that run IIS.

- In version 1802, this certificate is required in all scenarios. Only management points that you enable for CMG must be HTTPS. This change in behavior provides better support for Azure AD token-based authentication.

- Starting in version 1806, when using the site option to **Use Configuration Manager-generated certificates for HTTP site systems**, the management point can be HTTP. For more information, see Enhanced HTTP.

> **TIP**
> If you aren't using Enhanced HTTP, and your environment has multiple management points, you don't have to HTTPS-enable them all for CMG. Configure the CMG-enabled management points as **Internet only**. Then your on-premises clients don't try to use them.

Management point client connection mode summary

These tables summarize whether the management point requires HTTP or HTTPS, depending upon the type of client and site version.

For internet-based clients communicating with the cloud management gateway

Configure an on-premises management point to allow connections from the CMG with the following client connection mode:

TYPE OF CLIENT	1802	1806	1810
Workgroup	HTTPS	E-HTTP[Note 1], HTTPS	E-HTTP[Note 1], HTTPS
AD domain-joined	HTTPS	E-HTTP[Note 1], HTTPS	E-HTTP[Note 1], HTTPS
Azure AD-joined	HTTPS	E-HTTP, HTTPS	E-HTTP, HTTPS
Hybrid-joined	HTTPS	E-HTTP, HTTPS	E-HTTP, HTTPS

> **NOTE**
> **Note 1**: This configuration requires the client has a client authentication certificate, and only supports device-centric scenarios.

For on-premises clients communicating with the on-premises management point

Configure an on-premises management point with the following client connection mode:

TYPE OF CLIENT	1802	1806	1810
Workgroup	HTTP, HTTPS	HTTP, HTTPS	HTTP, HTTPS
AD domain-joined	HTTP, HTTPS	HTTP, HTTPS	HTTP, HTTPS
Azure AD-joined	HTTPS	HTTPS	HTTPS
Hybrid-joined	HTTP, HTTPS	HTTP, HTTPS	HTTP, HTTPS

> **NOTE**
>
> In version 1806, AD domain-joined clients support both device- and user-centric scenarios communicating with an HTTP or HTTPS management point.
>
> Azure AD-joined and hybrid-joined clients can communicate via HTTP for device-centric scenarios, but need E-HTTP or HTTPS to enable user-centric scenarios. Otherwise they behave the same as workgroup clients.

Legend of terms

- *Workgroup*: The device isn't joined to a domain or Azure AD, but has a client authentication certificate
- *AD domain-joined*: You join the device to an on-premises Active Directory domain
- *Azure AD-joined*: Also known as cloud domain-joined, you join the device to an Azure Active Directory tenant
- *Hybrid-joined*: You join the device to both an Active Directory domain and an Azure AD tenant
- *HTTP*: On the management point properties, you set the client connections to **HTTP**
- *HTTPS*: On the management point properties, you set the client connections to **HTTPS**
- *E-HTTP*: On the site properties, **Client Computer Communication** tab, you set the site system settings to **HTTPS or HTTP**, and you enable the option to **Use Configuration Manager-generated certificates for HTTP site systems**. You configure the management point for HTTP, the HTTP management point is ready for both HTTP and HTTPS communication (token auth scenarios).

  > **NOTE**
  >
  > Starting in version 1906, this tab is called **Communication Security**.

Azure management certificate

This certificate is required for classic service deployments. It's not required for Azure Resource Manager deployments.

> **IMPORTANT**
>
> Starting in version 1810, classic service deployments in Azure are deprecated in Configuration Manager. Start using Azure Resource Manager deployments for the cloud management gateway. For more information, see Plan for CMG.
>
> Starting in Configuration Manager version 1902, Azure Resource Manager is the only deployment mechanism for new instances of the cloud management gateway. This certificate isn't required in Configuration Manager version 1902 or later.

You supply this certificate in the Azure portal, and when creating the CMG in the Configuration Manager console.

To create the CMG in Azure, the Configuration Manager service connection point needs to first authenticate to your Azure subscription. When using a classic service deployment, it uses the Azure management certificate for this authentication. An Azure administrator uploads this certificate to your subscription. When you create the CMG in the Configuration Manager console, provide this certificate.

For more information and instructions for how to upload a management certificate, see the following articles in the Azure documentation:

- Cloud services and management certificates
- Upload an Azure Service Management Certificate

IMPORTANT

Make sure to copy the subscription ID associated with the management certificate. You use it for creating the CMG in the Configuration Manager console.

Next steps

- Set up cloud management gateway
- Frequently asked questions about the cloud management gateway
- Security and privacy for cloud management gateway

Set up cloud management gateway for Configuration Manager

7/26/2019 • 12 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This process includes the steps required to set up a cloud management gateway (CMG).

> **NOTE**
> Configuration Manager doesn't enable this optional feature by default. You must enable this feature before using it. For more information, see Enable optional features from updates.

Before you begin

Start by reading the article Plan for cloud management gateway. Use that article to determine your CMG design.

Use the following checklist to make sure you have the necessary information and prerequisites to create a CMG:

- The Azure environment to use. For example, the Azure Public Cloud or the Azure US Government Cloud.
- You need one or more certificates for CMG, depending upon your design. For more information, see Certificates for cloud management gateway.
- You need the following requirements for an Azure Resource Manager deployment of CMG:
  - Integration with Azure AD for **Cloud Management**. Azure AD user discovery isn't required.
  - The **Microsoft.ClassicCompute** & **Microsoft.Storage** resource providers must be registered within the Azure subscription. For more information, see Azure Resource Manager.
  - A subscription admin needs to sign in.
- A globally unique name for the service. This name is from the CMG server authentication certificate.
- If enabling CMG as a cloud distribution point, the same globally unique CMG service name chosen also needs to be available as a globally unique storage account name. This name is from the CMG server authentication certificate.
- The Azure region for this CMG deployment.
- How many VM instances you need for scale and redundancy.
- If you still need to use the Azure classic service deployment in Configuration Manager version 1810 or earlier, you need the following requirements:

> **IMPORTANT**
> Starting in version 1810, classic service deployments in Azure are deprecated in Configuration Manager. Use Azure Resource Manager deployments for the cloud management gateway. For more information, see Plan for CMG.
>
> Starting in Configuration Manager version 1902, Azure Resource Manager is the only deployment mechanism for new instances of the cloud management gateway.

- Azure subscription ID
- Azure management certificate

Set up a CMG

Do this procedure on the top-level site. That site is either a standalone primary site, or the central administration site.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Cloud Services**, and select **Cloud Management Gateway**.
2. Select **Create Cloud Management Gateway** in the ribbon.
3. On the General page of the wizard, select **Sign in**. Authenticate with an Azure subscription administrator account. The wizard auto-populates the remaining fields from the information stored during the Azure AD integration prerequisite. If you own multiple subscriptions, select the **Subscription ID** of the desired subscription to use.

   > **NOTE**
   >
   > Starting in version 1810, classic service deployments in Azure were deprecated in Configuration Manager. In version 1902 and earlier, select **Azure Resource Manager deployment** as the CMG deployment method.
   >
   > If you need to use a classic service deployment, select that option on this page. First enter your Azure **Subscription ID**. Then select **Browse**, and choose the .PFX file for the Azure management certificate.

4. Specify the **Azure environment** for this CMG. The options in the drop-down list may vary depending upon the deployment method.
5. Select **Next**. Wait as the site tests the connection to Azure.
6. On the Settings page of the wizard, first select **Browse** and choose the .PFX file for the CMG server authentication certificate. The name from this certificate populates the required **Service FQDN** and **Service name** fields.

   > **NOTE**
   >
   > The CMG server authentication certificate supports wildcards. If you use a wildcard certificate, replace the asterisk (`*`) in the **Service FQDN** field with the desired hostname for the CMG.

7. Select the **Region** drop-down list to choose the Azure region for this CMG.
8. Select a **Resource Group** option.
   a. If you choose **Use existing**, then select an existing resource group from the drop-down list. The selected resource group must already exist in the region you selected in step 7. If you select an existing resource group and it is in a different region than the previously selected region, CMG will fail to provision.
   b. If you choose **Create new**, then enter the new resource group name.
9. In the **VM Instance** field, enter the number of VMs for this service. The default is one, but you can scale up to 16 VMs per CMG.
10. Select **Certificates** to add client trusted root certificates. Add all of the certificates in the trust chain.

> **NOTE**
>
> Starting in version 1806, when you create a CMG, you're no longer required to provide a trusted root certificate on the Settings page. This certificate isn't required when using Azure Active Directory (Azure AD) for client authentication, but used to be required in the wizard. If you're using PKI client authentication certificates, then you still must add a trusted root certificate to the CMG.
>
> In version 1902 and earlier, you can only add two trusted root CAs and four intermediate (subordinate) CAs.

11. By default, the wizard enables the option to **Verify Client Certificate Revocation**. A certificate revocation list (CRL) must be publicly published for this verification to work. For more information, see Publish the certificate revocation list.

12. Starting in version 1906, you can **Enforce TLS 1.2**. This setting only applies to the Azure cloud service VM. It doesn't apply to any on-premises Configuration Manager site servers or clients. For more information on TLS 1.2, see How to enable TLS 1.2.

13. Starting in version 1806, by default, the wizard enables the following option: **Allow CMG to function as a cloud distribution point and serve content from Azure storage**. Now a CMG can also serve content to clients. This functionality reduces the required certificates and cost of Azure VMs.

14. Select **Next**.

15. To monitor CMG traffic with a 14-day threshold, choose the check box to turn on the threshold alert. Then, specify the threshold, and the percentage at which to raise the different alert levels. Choose **Next** when you're done.

16. Review the settings, and choose **Next**. Configuration Manager starts setting up the service. After you close the wizard, it will take between five to 15 minutes to provision the service completely in Azure. Check the **Status** column for the new CMG to determine when the service is ready.

> **NOTE**
>
> To troubleshoot CMG deployments, use **CloudMgr.log** and **CMGSetup.log**. For more information, see Log files.

Configure primary site for client certificate authentication

If you're using client authentication certificates for clients to authenticate with the CMG, follow this procedure to configure each primary site.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select **Sites**.

2. Select the primary site to which your internet-based clients are assigned, and choose **Properties**.

3. Switch to the **Client Computer Communication** tab of the primary site property sheet, check **Use PKI client certificate (client authentication) when available**.

> **NOTE**
>
> Starting in version 1906, this tab is called **Communication Security**.

4. If you don't publish a CRL, deselect the option for **Clients check the certificate revocation list (CRL) for site systems**.

Add the CMG connection point

The CMG connection point is the site system role for communicating with the CMG. To add the CMG connection point, follow the general instructions to install site system roles. On the System Role Selection page of the Add Site System Role Wizard, select **Cloud management gateway connection point**. Then select the **Cloud management gateway name** to which this server connects. The wizard shows the region for the selected CMG.

> **IMPORTANT**
> The CMG connection point must have a client authentication certificate in some scenarios.

To troubleshoot CMG service health, use **CMGService.log** and **SMS_Cloud_ProxyConnector.log**. For more information, see Log files.

Configure client-facing roles for CMG traffic

Configure the management point and software update point site systems to accept CMG traffic. Do this procedure on the primary site, for all management points and software update points that service internet-based clients.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and select the **Servers and Site System Roles** node. On the Home tab of the ribbon, in the View group, select **Servers with Role**. Then select **Management point** from the list.
2. Select the site system server you want to configure for CMG traffic. Select the **Management point** role in the details pane, and then select **Properties** in the ribbon.
3. In the Management point properties sheet under Client Connections, check the box next to **Allow Configuration Manager cloud management gateway traffic**.

   Depending upon your CMG design and Configuration Manager version, you may need to enable the **HTTPS** option. For more information, see Enable management point for HTTPS.
4. Select **OK** to close the management point properties window.

Repeat these steps for additional management points as needed, and for any software update points.

Configure boundary groups

Starting in version 1902, you can associate a CMG with a boundary group. This configuration allows clients to default or fallback to the CMG for client communication according to boundary group relationships.

For more information on boundary groups, see Configure boundary groups.

When you create or configure a boundary group, on the **References** tab, add a cloud management gateway. This action associates the CMG with this boundary group.

Configure clients for CMG

Once the CMG and site system roles are running, clients get the location of the CMG service automatically on the next location request. Clients must be on the intranet to receive the location of the CMG service, unless you install and assign Windows 10 clients using Azure AD for authentication. The polling cycle for location requests is every 24 hours. If you don't want to wait for the normally scheduled location request, you can force the request by restarting the SMS Agent Host service (ccmexec.exe) on the computer.

> **NOTE**
>
> By default all clients receive CMG policy. Control this behavior with the client setting, Enable clients to use a cloud management gateway.

The Configuration Manager client automatically determines whether it's on the intranet or the internet. If the client can contact a domain controller or an on-premises management point, it sets its connection type to **Currently intranet**. Otherwise, it switches to **Currently Internet**, and uses the location of the CMG service to communicate with the site.

> **NOTE**
>
> You can force the client to always use the CMG regardless of whether it's on the intranet or internet. This configuration is useful for testing purposes, or for clients at remote offices that you want to force to use the CMG. Set the following registry key on the client:
>
> `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM\Security, ClientAlwaysOnInternet = 1`
>
> You can also specify this setting during client installation using the CCMALWAYSINF property.

To verify that clients have the policy specifying the CMG, open a Windows PowerShell command prompt as an administrator on the client computer, and run the following command:

```
Get-WmiObject -Namespace Root\Ccm\LocationServices -Class SMS_ActiveMPCandidate | Where-Object {$_.Type -eq "Internet"}
```

This command displays any internet-based management points the client knows about. While the CMG isn't technically an internet-based management point, clients view it as one.

> **NOTE**
>
> To troubleshoot CMG client traffic, use **CMGHttpHandler.log**, **CMGService.log**, and **SMS_Cloud_ProxyConnector.log**. For more information, see Log files.

Modify a CMG

After creating a CMG, you can modify some of its settings. Select the CMG in the Configuration Manager console and select **Properties**. Configure settings on the following tabs:

General

- **Azure management certificate**: change the Azure management certificate for the CMG. This option is useful when updating the certificate before it expires.

Settings

- **Certificate file**: change the server authentication certificate for the CMG. This option is useful when updating the certificate before it expires.
- **VM Instance**: change the number of virtual machines that the service uses in Azure. This setting allows you to dynamically scale the service up or down based on utilization or cost considerations.
- **Certificates**: add or remove trusted root or intermediate CA certificates. This option is useful when adding new CAs, or retiring expired certificates.
- **Verify Client Certificate Revocation**: if you didn't originally enable this setting when creating the CMG, you can enable it afterwards once you publish the CRL. For more information, see Publish the certificate revocation list.

- **Allow CMG to function as a cloud distribution point and serve content from Azure storage**: Starting in version 1806, this new option is enabled by default. Now a CMG can also serve content to clients. This functionality reduces the required certificates and cost of Azure VMs.

Alerts

Reconfigure the alerts at anytime after you create the CMG.

Redeploy the service

More significant changes, such as the following configurations, require redeploying the service:

- Classic deployment method to Azure Resource Manager
- Subscription
- Service name
- Private to public PKI
- Region

Always keep at least one active CMG for internet-based clients to receive updated policy. internet-based clients can't communicate with a removed CMG. Clients don't know about a new one until they roam back to the intranet. When creating a second CMG instance in order to delete the first, also create another CMG connection point.

Clients refresh policy by default every 24 hours, so wait at least one day after creating a new CMG before you delete the old one. If clients are turned off or without an internet connection, you may need to wait longer.

If you have an existing CMG on the classic deployment method, you must deploy a new CMG to use the Azure Resource Manager deployment method. There are two options:

- If you want to reuse the same service name:
  1. First delete the classic CMG, taking into account the guidance to always have at least one active CMG for internet-based clients.
  2. Create a new CMG using a Resource Manager deployment. Reuse the same server authentication certificate.
  3. Reconfigure the CMG connection point to use the new CMG instance.
- If you want to use a new service name:
  1. Create a new CMG using a Resource Manager deployment. Use a new server authentication certificate.
  2. Create a new CMG connection point and link with the new CMG.
  3. Wait at least one day for internet-based clients to receive policy about the new CMG.
  4. Delete the classic CMG.

> **TIP**
>
> To determine the current deployment model of a CMG:
>
> 1. In the Configuration Manager console, go to the **Administration** workspace, expand **Cloud Services**, and select the **Cloud Management Gateway** node.
> 2. Select the CMG instance.
> 3. In the Details pane at the bottom of the window, look for the **Deployment Model** attribute. For a Resource Manager deployment, this attribute is **Azure Resource Manager**. The legacy deployment model with the Azure management certificate displays as **Azure Service Manager**.
>
> You can also add the **Deployment Model** attribute as a column to the list view.

Modifications in the Azure portal

Only modify the CMG from the Configuration Manager console. Making modifications to the service or underlying VMs directly in Azure isn't supported. Any changes may be lost without notice. As with any PaaS, the service can rebuild the VMs at anytime. These rebuilds can happen for backend hardware maintenance, or to apply updates to the VM OS.

Delete the service

If you need to delete the CMG, also do so from the Configuration Manager console. Manually removing any components in Azure causes the system to be inconsistent. This state leaves orphaned information, and unexpected behaviors may occur.

Next steps

- Monitor clients for cloud management gateway
- Frequently asked questions about the cloud management gateway

Monitor cloud management gateway

6/20/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

After the cloud management gateway (CMG) is running and clients are connecting through it, you can monitor clients and network traffic to make sure you know how the service is performing.

Monitor clients

Clients connected through the CMG appear in the Configuration Manager console the same way on-premises clients do. For more information, see how to monitor clients.

Monitor traffic in the console

Monitor traffic on the CMG using the Configuration Manager console:

1. Go to the **Administration** workspace, expand **Cloud Services**, and select the **Cloud Management Gateway** node.
2. Select the CMG in the list pane.
3. View the traffic information in the details pane for the CMG connection point and the site system roles it connects to. These statistics show the client requests coming into these roles. The requests include policy, location, registration, content, inventory, and client notifications.

Set up outbound traffic alerts

Outbound traffic alerts help you know when network traffic approaches a 14-day threshold level. When you create the CMG, you can set up traffic alerts. If you skipped that part, you can still set up the alerts after the service is running. Adjust the alert settings at any time.

1. Go to the **Administration** workspace, expand **Cloud Services**, and select the **Cloud Management Gateway** node.
2. Select the CMG in the list pane, and then select **Properties** in the ribbon.
3. Go to the **Alerts** tab to enable the threshold and alerts. Specify the 14-day data threshold in gigabytes (GB). Also specify the threshold percentage to raise the different alert levels.
4. When you're done, select **OK**.

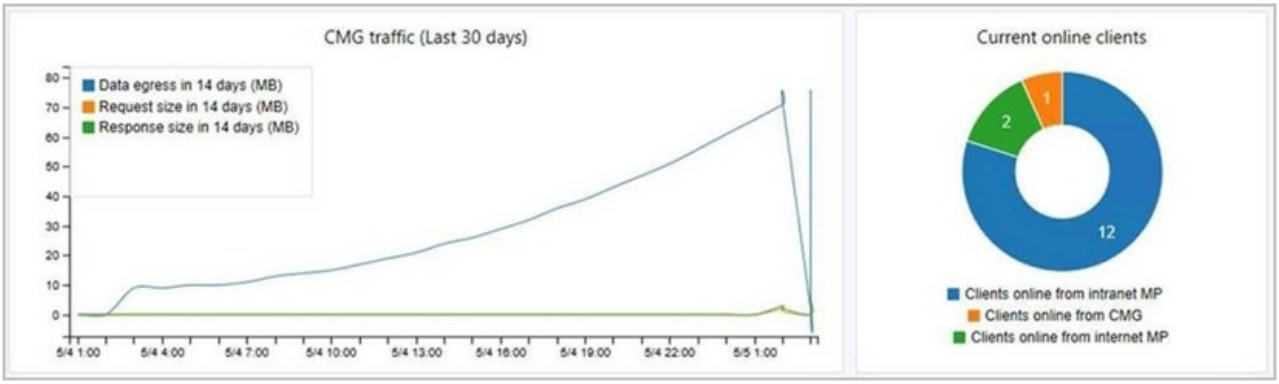
Monitor logs

The CMG generates entries in a number of log files. For more information, see Configuration Manager logs.

Cloud management dashboard

Starting in version 1806, the cloud management dashboard provides a centralized view for CMG usage. When the site is onboarded to Azure services for cloud management, it also displays data about cloud users and devices.

The following screenshot is a portion of the cloud management dashboard showing two of the available tiles:



In the Configuration Manager console, go to the **Monitoring** workspace. Select the **Cloud Management** node, and view the dashboard tiles.

Connection analyzer

Starting in version 1806, use the CMG connection analyzer for real-time verification to aid troubleshooting. The in-console utility checks the current status of the service, and the communication channel through the CMG connection point to any management points that allow CMG traffic.

1. In the Configuration Manager console, go to the **Administration** workspace. Expand **Cloud Services** and select the **Cloud management gateway** node.
2. Select the target CMG instance, and then select **Connection analyzer** in the ribbon.
3. In the CMG connection analyzer window, select one of the following options to authenticate with the service:
   a. **Azure AD user**: use this option to simulate communication the same as a cloud-based user identity signed in to an Azure AD-joined Windows 10 device. Click **Sign In** to securely enter the credentials for this Azure AD user account.
   b. **Client certificate**: use this option to simulate communication the same as a Configuration Manager client with a client authentication certificate.
4. Select **Start** to start the analysis. The analyzer window displays the results. Select an entry to see more details in the Description field.

Stop CMG when it exceeds threshold

Starting in version 1902, Configuration Manager can now stop a CMG service when the total data transfer goes over your limit. Use alerts to trigger notifications when the usage reaches warning or critical levels. To help reduce any unexpected Azure costs because of a spike in usage, this option turns off the cloud service.

> **IMPORTANT**
> Even if the service isn't running, there are still costs associated with the cloud service. Stopping the service doesn't eliminate all associated Azure costs. To remove all cost for the cloud service, remove the CMG.
>
> When the CMG service is stopped, internet-based clients can't communicate with Configuration Manager.

The total data transfer (egress) includes data from the cloud service and storage account. This data comes from the following flows:

- CMG to client
- CMG to site, including CMG log files
- If you enable CMG for content, storage account to client

For more information on these data flows, see CMG ports and data flow.

The storage alert threshold is separate. That alert monitors the capacity of your Azure storage instance.

When you select the CMG instance in the **Cloud Management Gateway** node in the console, you can see the total data transfer in the details pane.

Configuration Manager checks the threshold value every six minutes. If there's a sudden spike in usage, Configuration Manager can take up to six minutes to detect that it exceeded the threshold and then stop the service.

Process to stop the cloud service when it exceeds threshold

1. Set up outbound traffic alerts.
2. On the **Alerts** tab of the CMG properties window, enable the option to **Stop this service when the critical threshold is exceeded**.

To test this feature, temporarily reduce one of the following values:

- **14-day threshold for outbound data transfer (GB)**. The default value is `10000`.
- **Percentage of threshold for raising Critical alert**. The default value is `90`.

Plan for internet-based client management in System Center Configuration Manager

9/5/2019 • 10 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Internet-based client management (sometimes referred to as IBCM) lets you manage System Center Configuration Manager clients when they are not connected to your company network but have a standard internet connection. This arrangement has several advantages that include the reduced costs of not having to run virtual private networks (VPNs) and being able to deploy software updates in a timelier manner.

Because of the higher security requirements of managing client computers on a public network, internet-based client management requires that clients and the site system servers that the clients connect to use PKI certificates. This ensures that connections are authenticated by an independent authority, and that data to and from these site systems are encrypted by using Secure Sockets Layer (SSL).

Use the following sections to help you plan for internet-based client management.

Features that Are Not Supported on the internet

Not all client management functionality is appropriate for the internet; therefore they are not supported when clients are managed on the internet. The features that are not supported for internet management typically rely on Active Directory Domain Services or are not appropriate for a public network, such as network discovery and Wake-on-LAN (WOL).

The following features are not supported when clients are managed on the internet:

- Client deployment over the internet, such as client push and software update-based client deployment. Instead, use manual client installation.
- Automatic site assignment.
- Wake-on-LAN.
- Operating system deployment. However, you can deploy task sequences that do not deploy an operating system; for example, task sequences that run scripts and maintenance tasks on clients.
- Remote control.
- Software deployment to users unless the internet-based management point can authenticate the user in Active Directory Domain Services by using Windows authentication (Kerberos or NTLM). This is possible when the internet-based management point trusts the forest where the user account resides.

  Additionally, internet-based client management does not support roaming. Roaming enables clients to always find the closest distribution points to download content. Clients that are managed on the internet communicate with site systems from their assigned site when these site systems are configured to use an internet FQDN and the site system roles allow client connections from the internet. Clients non-deterministically select one of the internet-based site systems, regardless of bandwidth or physical location.

  When you have a software update point that is configured to accept connections from the internet, Configuration Manager internet-based clients on the internet always scan against this software update point, to determine which software updates are required. However, when these clients are on the internet, they first try to download the software updates from Microsoft Update, rather than from an internet-based

distribution point. Only if this fails, will they then try to download the required software updates from an internet-based distribution point. Clients that are not configured for internet-based client management never try to download the software updates from Microsoft Update, but always use Configuration Manager distribution points.

> **TIP**
> The Configuration Manager client automatically determines whether it's on the intranet or the internet. If the client can contact a domain controller or an on-premises management point, it sets its connection type to Currently intranet. Otherwise, it switches to Currently internet, and the client uses the management points, software update points, and distribution points assigned to its site for communication.

Considerations for client communications from the internet or untrusted forest

The following site system roles installed at primary sites support connections from clients that are in untrusted locations, like the internet or an untrusted forest (secondary sites do not support client connections from untrusted locations):

- Application Catalog website point

  > **IMPORTANT**
  > The application catalog is deprecated. For more information, see Remove the application catalog.

- Configuration Manager Policy Module
- Distribution point (HTTPS is required by cloud-based distribution points)
- Enrollment proxy point
- Fallback status point
- Management point
- Software update point

  About internet facing site systems:
  Although there is no requirement to have a trust between a client's forest and that of the site system server, when the forest that contains an internet facing site system trusts the forest that contains the user accounts, this configuration supports user-based policies for devices on the internet when you enable the **Client Policy** client setting **Enable user policy requests from internet clients**.

  For example, the following configurations illustrate when internet-based client management supports user policies for devices on the internet:

- The internet-based management point is in the perimeter network where a read-only domain controller resides to authenticate the user and an intervening firewall allows Active Directory packets.
- The user account is in Forest A (the intranet) and the internet-based management point is in Forest B (the perimeter network). Forest B trusts Forest A, and an intervening firewall allows the authentication packets.
- The user account and the internet-based management point are in Forest A (the intranet). The management point is published to the internet by using a web proxy server (like Forefront Threat Management Gateway).

> **NOTE**
> If Kerberos authentication fails, NTLM authentication is then automatically tried.

As the previous example shows, you can place internet-based site systems in the intranet when they are published to the internet by using a web proxy server, such as ISA Server and Forefront Threat Management Gateway. These site systems can be configured for client connection from the internet only, or client connections from the internet and intranet. When you use a web proxy server, you can configure it for Secure Sockets Layer (SSL) bridging to SSL (more secure) or SSL tunneling:

- **SSL bridging to SSL:**
  The recommended configuration when you use proxy web servers for internet-based client management is SSL bridging to SSL, which uses SSL termination with authentication. Client computers must be authenticated by using computer authentication, and mobile device legacy clients are authenticated by using user authentication. Mobile devices that are enrolled by Configuration Manager do not support SSL bridging.

  The benefit of SSL termination at the proxy web server is that packets from the internet are subject to inspection before they are forwarded to the internal network. The proxy web server authenticates the connection from the client, terminates it, and then opens a new authenticated connection to the internet-based site systems. When Configuration Manager clients use a proxy web server, the client identity (client GUID) is securely contained in the packet payload so that the management point does not consider the proxy web server to be the client. Bridging is not supported in Configuration Manager with HTTP to HTTPS, or from HTTPS to HTTP.

  > **NOTE**
  > Configuration Manager doesn't support setting third-party SSL bridging configurations. For example, Citrix Netscaler or F5 BIG-IP. Please work with your device vendor to configure it for use with Configuration Manager.

- **Tunneling**:
  If your proxy web server cannot support the requirements for SSL bridging, or you want to configure internet support for mobile devices that are enrolled by Configuration Manager, SSL tunneling is also supported. It is a less secure option because the SSL packets from the internet are forwarded to the site systems without SSL termination, so they cannot be inspected for malicious content. When you use SSL tunneling, there are no certificate requirements for the proxy web server.

Planning for internet-Based Clients

You must decide whether the client computers that will be managed over the internet will be configured for management on the intranet and the internet, or for internet-only client management. You can only configure the client management option during the installation of a client computer. If you change your mind later, you must reinstall the client.

> **NOTE**
> If you configure an internet capable management point, clients that connect to the management point will become internet-capable when they next refresh their list of available management points.

> **TIP**
> You do not have to restrict the configuration of internet-only client management to the internet and you can also use it on the intranet.

Clients that are configured for internet-only client management only communicate with the site systems that are configured for client connections from the internet. This configuration would be appropriate for computers that you know never connect to your company intranet, for example, point of sale computers in remote locations. It might also be appropriate when you want to restrict client communication to HTTPS only (for example, to support firewall and restricted security policies), and when you install internet-based site systems in a perimeter network and you want to manage these servers by using the Configuration Manager client.

When you want to manage workgroup clients on the internet, you must install them as internet-only.

> **NOTE**
> Mobile device clients are automatically configured as internet-only when they are configured to use an internet-based management point.

Other client computers can be configured for internet and intranet client management. They can automatically switch between internet-based client management and intranet client management when they detect a change of network. If these clients can find and connect to a management point that is configured for client connections on the intranet, these clients are managed as intranet clients that have full Configuration Manager management functionality. If the clients cannot find or connect to a management point that is configured for client connections on the intranet, they attempt to connect to an internet-based management point, and if this is successful, these clients are then managed by the internet-based site systems in their assigned site.

The benefit in automatic switching between internet-based client management and intranet client management is that client computers can automatically use all Configuration Manager features whenever they are connected to the intranet and continue to be managed for essential management functions when they are on the internet. Additionally, a download that began on the internet can seamlessly resume on the intranet, and vice versa.

Prerequisites for internet-Based Client Management

Internet-based client management in Configuration Manager has the following external dependencies:

- Clients that will be managed on the internet must have an internet connection.

  Configuration Manager uses existing Internet Service Provider (ISP) connections to the internet, which can be either permanent or temporary connections. Client mobile devices must have a direct internet connection, but client computers can have either a direct internet connection or connect by using a proxy web server.

- Site systems that support internet-based client management must have connectivity to the internet and must be in an Active Directory domain.

  The internet-based site systems do not require a trust relationship with the Active Directory forest of the site server. However, when the internet-based management point can authenticate the user by using Windows authentication, user policies are supported. If Windows authentication fails, only computer policies are supported.

> **NOTE**
>
> To support user policies, you also must set to **True** the two **Client Policy** client settings:
>
> - **Enable user policy polling on clients**
>   - **Enable user policy requests from Internet clients**

An internet-based Application Catalog website point also requires Windows authentication to authenticate users when their computer is on the internet. This requirement is independent from user policies.

- You must have a supporting public key infrastructure (PKI) that can deploy and manage the certificates that the clients require and that are managed on the internet and the internet-based site system servers.

  For more information about the PKI certificates, see PKI certificate requirements for System Center Configuration Manager.

- The internet fully qualified domain name (FQDN) of site systems that support internet-based client management must be registered as host entries on public DNS servers.

- Intervening firewalls or proxy servers must allow the client communication that is associated with internet-based site systems.

  Client communication requirements:

  - Support HTTP 1.1
  - Allow HTTP content type of multipart MIME attachment (multipart/mixed and application/octet-stream)
  - Allow the following verbs for the internet-based management point:
    - HEAD
    - CCM_POST
    - BITS_POST
    - GET
    - PROPFIND
  - Allow the following verbs for the internet-based distribution point:
    - HEAD
    - GET
    - PROPFIND
  - Allow the following verbs for the internet-based fallback status point:
    - POST
  - Allow the following verbs for the internet-based Application Catalog website point:
    - POST
    - GET
  - Allow the following HTTP headers for the internet-based management point:
    - Range:

- CCMClientID:
- CCMClientIDSignature:
- CCMClientTimestamp:
- CCMClientTimestampsSignature:

- Allow the following HTTP header for the internet-based distribution point:
  - Range:

  For configuration information to support these requirements, refer to your firewall or proxy server documentation.

  For similar communication requirements when you use the software update point for client connections from the internet, see the documentation for Windows Server Update Services (WSUS). For example, for WSUS on Windows Server 2003, see Appendix D: Security Settings, the deployment appendix for security settings.

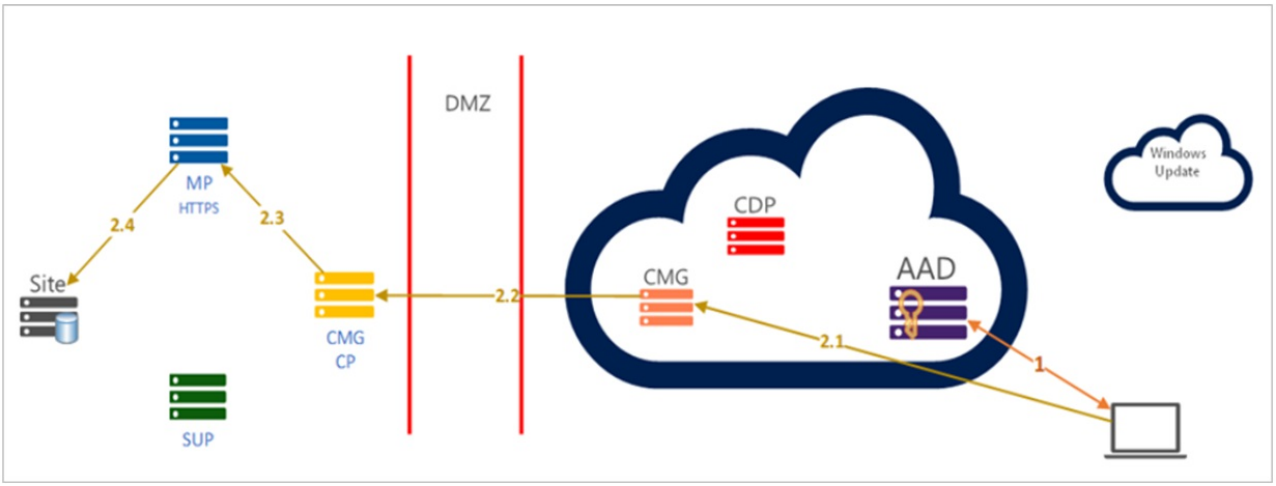
Azure AD authentication workflow

9/11/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article is a technical reference for the Configuration Manager client installation process on a Windows 10 device that's joined to Azure Active Directory (Azure AD). It details the workflow process for the device authentication and client installation.

Azure AD token request workflow



1. Azure AD token request

A Windows 10 Azure AD domain-joined client uses Azure AD parameters to request a token. The following entries are logged in **ccmsetup.log**:

- Request Azure AD device token:

```
Getting AAD (device) token with: ClientId = 22ed38d9-XXXX-4036-XXXX-a98452fda4fc, ResourceUrl =
https://ConfigMgrService, AccountId = https://login.microsoftonline.com/common/oauth2/token
```

- If it can't get a device token, it requests an Azure AD user token:

```
Getting AAD (user) token with: ClientId = f1f9b14e-XXXX-4f17-XXXX-2593f6eee91e, ResourceUrl =
https://ConfigMgrService, AccountId = X49FC29A-ECE3-XXX-A3C1-XXXXXXF035A6E
```

> **NOTE**
>
> A client should get a workplace join (WPJ) certificate when it joins Azure AD. If a workplace join certificate isn't found, the client doesn't try to create the request using the Security Token Service communication channel (CCM_STS). This behavior is because the client can't add an Azure AD token to the request. The device typically doesn't have this certificate when the client isn't properly joined to Azure AD.
>
> Additionally, if the token isn't valid, the cloud management gateway (CMG) doesn't forward the request to the internal site roles. The token can be invalid if the tenant isn't registered as a cloud management service in Configuration Manager.

2. Configuration Manager client token request

Once the client has an Azure AD token, it requests a Configuration Manager client (CCM) token.

The following entries are logged in **ccmsetup.log** of the CMG virtual machine:

```
Getting CCM Token from STS server 'CloudManagementGateway.cloudapp.net/CCM_PROXY_MUTUALAUTH/XXXXXX037938216'
Getting CCM Token from https://CloudManagementGateway.cloudapp.net/CCM_PROXY_MUTUALAUTH/XXXXXX037938216/CCM_STS
```

2.1 CMG gets request

The following entries are logged in **IIS.log**:

```
RD0003FF74XX2 10.0.0.4 GET /CCM_STS - 443 - HTTP/1.1 python-requests/2.20.0 - - 13.95.234.44 404 0 2 1477 154
15
```

2.2 CMG forwards request to CMG connection point

The following entries are logged in **CMGService.log**:

```
RequestUri: /CCM_PROXY_SERVERAUTH/XXXXXX037938216/CCM_STS  RequestCount: 769  RequestSize: 1081595 Bytes
ResponseCount: 769     ResponseSize: 36143 Bytes  AverageElapsedTime: 3945 ms
```

2.3 CMG connection point transforms CMG client request to management point client request

The following entries are logged in **SMS_CLOUD_PROXYCONNECTOR.log**:

```
MessageID: 3087bd34-b82c-4950-b972-e82bb0fb8385 RequestURI: https://MP.MYCORP.COM/CCM_STS EndpointName: CCM_STS
ResponseHeader: HTTP/1.1 200 OK ~~ ResponseBodySize: 0 ElapsedTime: 2 ms
```

2.4 Management point verifies user token in site database

The following entries are logged in **CCM_STS.log**:

```
Validated AAD token. TokenType: Device TenantId: XXXXe388-XXXX-485c-XXXX-e8e4eb41XXXX UserId: 00000000-0000-
0000-0000-000000000000 DeviceId: 0XXXXX80-77XX-4XXa-X63X-67XXXXX64bb7 OnPrem_UserSid:  OnPrem_DeviceSid:

Return token to client, token type: UDA, hierarchyId: XXXX4f9c-XXXX-46a5-XXXX-7612c324XXXX, userId: 00000000-
0000-0000-0000-000000000000, deviceId: GUID:XXXXaee9-cXXc-4ccd-XXXX-f1417d81XXX
```

Content location request

Once the client gets a response with the CCM token, it caches and uses it to request site information and content location through the CMG. The following entries are logged in **ccmsetup.log**:

```
Cached encrypted token for 'S-1-5-18'. Will expire at '00/99/2999 00:00:00'
Sending location request to 'CloudManagementGateway.cloudapp.net/CCM_PROXY_MUTUALAUTH/XXXXXX037938216' with
payload '< Request >
Appending CCM Token to the header.
```

Client installation

The device downloads the client content and starts the installation.

Communication validation

- CMG validates client token via CMG, CMG connection point and HTTP(S), and management point database request.
- Client verifies CMG service certificate or management certificate

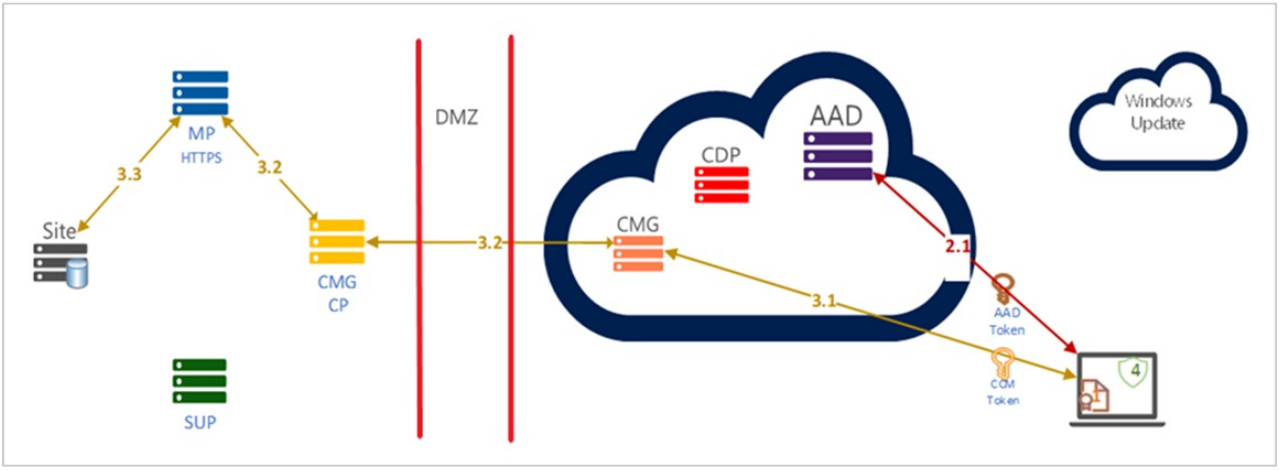
- PKI for CMG service certificate: Client requires root certificate authority (CA) of the CMG certificate on local store
- Third-party CMG service certificate: Clients automatically validate a certificate with its root CA published on the internet

Common issues

- Root CA not present
- CRL check enabled: publish CRL on internet, or use the **/NoCRLcheck** option in command line
- WPJ certificate not found: client is registered with Azure AD, but not joined to Azure AD

Using /NoCRLCheck is only good for ccmsetup bootstrap. For the clients to be fully functional, you should publish the CRL on the internet. As a workaround, you can disable the CRL check on the site's client communication configuration. Otherwise, after the security settings are refreshed by location service, the clients stop communicating with the server.

Client registration



1. Configuration Manager client request registration

The following entries are logged in **ClientIDManagerStartup.log**:

```
[RegTask] - Client is not registered. Sending registration request for GUID:1XXXXXEF-5XX8-4XX3-XEDX-
XXXFBFF78XXX ...
Registering client using AAD auth.
```

2. Configuration Manager request Azure AD token to register client

The following entries are logged in **ADALOperationProvider.log**:

```
Getting AAD (user) token with: ClientId = f1f9b14e-XXXX-4f17-XXXX-2593f6eee91e, ResourceUrl =
https://ConfigMgrService, AccountId = X49FC29A-ECE3-XXX-A3C1-XXXXXXF035A6E
Retrieved AAD token for AAD user '00000000-0000-0000-0000-000000000000'
```

2.1 Configuration Manager client is registered

The following entries are logged in **ClientIDManagerStartup.log**:

```
[RegTask] - Client is registered. Server assigned ClientID is GUID:1XXXXXEF-5XX8-4XX3-XEDX-XXXFBFF78XXX.
Approval status 3
```

> **NOTE**
>
> During client registration, certificate validation always runs. This process happens even if you're using the Azure AD authentication method to register the client.

3. Configuration Manager client token request

Once the site registers the client, the client requests a CCM token. The CCM token is encrypted for the local System account (S-1-5-18) and cached for eight hours. After eight hours, the token expires, and the client requests token renewal.

The following entries are logged in **ClientIDManagerStartup.log**:

```
Getting CCM Token from STS server 'MP.MYCORP.COM'
Getting CCM Token from https://MP.MYCORP.COM/CCM_STS
...
Cached encrypted token for 'S-1-5-18'. Will expire at 'XX/XX/XX XX:XX:XX'
```

3.1 CMG gets request

The following entries are logged in **IIS.log**:

```
RD0003FF74XX2 10.0.0.4 GET /CCM_STS - 443 - HTTP/1.1 python-requests/2.20.0 - - 13.95.234.44 404 0 2 1477 154
15
```

3.2 CMG forwards request to CMG connection point

The following entries are logged in **CMGService.log**:

```
RequestUri: /CCM_PROXY_SERVERAUTH/XXXXXX037938216/CCM_STS  RequestCount: 769  RequestSize: 1081595 Bytes
ResponseCount: 769     ResponseSize: 36143 Bytes  AverageElapsedTime: 3945 ms
```

3.3 CMG connection point transforms CMG client request to management point client request

The following entries are logged in **SMS_CLOUD_PROXYCONNECTOR.log**:

```
MessageID: 3087bd34-b82c-4950-b972-e82bb0fb8385 RequestURI: https://MP.MYCORP.COM/CCM_STS EndpointName: CCM_STS
ResponseHeader: HTTP/1.1 200 OK ~~ ResponseBodySize: 0 ElapsedTime: 2 ms
```

3.4 Management point verifies user token in site database

The following entries are logged in **CCM_STS.log**:

```
Validated AAD token. TokenType: Device TenantId: XXXXe388-XXXX-485c-XXXX-e8e4eb41XXXX UserId: 00000000-0000-
0000-0000-000000000000 DeviceId: 0XXXXX80-77XX-4XXa-X63X-67XXXXX64bb7 OnPrem_UserSid:  OnPrem_DeviceSid:

Return token to client, token type: UDA, hierarchyId: XXXX4f9c-XXXX-46a5-XXXX-7612c324XXXX, userId: 00000000-
0000-0000-0000-000000000000, deviceId: GUID:XXXXaee9-cXXc-4ccd-XXXX-f1417d81XXX
```

Introduction to collections in System Center Configuration Manager

5/8/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Collections help you organize resources into manageable units. You can create collections to match your client management needs, and to perform operations on multiple resources at one time.

Most management tasks rely on or require using one or more collections. Although you can use the built-in collection of All Systems, using it for management tasks is not a best practice. Create custom collections to more specifically identify the devices or users for a task.

Built-in and custom collections appear in the **User Collections** and **Device Collections** nodes in the **Assets and Compliance** workspace in the Configuration Manager console.

Collections that you have recently viewed appear in the **Users** node and in the **Devices** node in the **Assets and Compliance** workspace.

Here are some examples of collection use:

OPERATION	EXAMPLE
Grouping resources	You can create collections that group resources based on your organization's hierarchy. For example, you could create a collection of all computers in the "London Headquarters" Active Directory Organizational Unit (OU). For more information about how to create this type of collection, see How to create collections in System Center Configuration Manager. You could use this collection for operations such as configuring Endpoint Protection settings, configuring device power management settings, or installing the Configuration Manager client.
Application deployment	You can create a collection of all computers that do not have Microsoft Office 2013 installed and then deploy it to all computers in that collection. You can also use application requirements to perform this task. For more information, see How to create applications with System Center Configuration Manager.
Managing client settings	Although the default client settings in Configuration Manager apply to all devices and all users, you can create custom client settings that apply to a collection of devices or a collection of users. For example, if you want remote control to be available on all but a few devices, configure the default client settings to allow remote control and then configure custom client settings that do not allow remote control, and deploy those to the collection of exceptional clients.

OPERATION	EXAMPLE
Power management	You can configure specific power settings per collection.
Role-based administration	Use collections to control which groups of users have access to various functionality in the Configuration Manager console.
Maintenance Windows	With maintenance windows you can define a time period when various Configuration Manager operations can be carried out on members of a device collection.

Collection types in Configuration Manager

Configuration Manager has built-in collections for common operations, and you can also create custom collections.

Built-in collections

By default, Configuration Manager includes the following collections, which cannot be modified.

COLLECTION NAME	DESCRIPTION
All User Groups	Contains the user groups that are discovered by using Active Directory Security Group Discovery.
All Users	Contains the users who are discovered by using Active Directory User Discovery.
All Users and User Groups	Contains the All Users and the All User Groups collections. This collection contains the largest scope of user and user group resources.
All Desktop and Server Clients	Contains the server and desktop devices that have the Configuration Manager client installed. Membership is maintained by Heartbeat Discovery.
All Mobile Devices	Contains the mobile devices that are managed by Configuration Manager. Membership is restricted to those mobile devices that are successfully assigned to a site or discovered by the Exchange Server connector.
All Systems	Contains the All Desktop and Server Clients, the All Mobile Devices, and the All Unknown Computers collections, and all mobile devices that are enrolled by Microsoft Intune. This collection contains the largest scope of device resources.
All Unknown Computers	Contains generic computer records for multiple computer platforms. You can use this collection to deploy an operating system by using a task sequence and PXE boot, bootable media, or prestaged media.

Custom collections

When you create a custom collection in Configuration Manager, the membership of that collection is determined by one or more collection rules, as described in How to create collections in System Center Configuration Manager.

Prerequisites for collections in System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Collections in System Center Configuration Manager contain only dependencies within the product.

Configuration Manager dependencies

DEPENDENCY	MORE INFORMATION
Reporting services point	The reporting services point site system role must be installed before you can run reports for collections. For more information, see Reporting in System Center Configuration Manager.
Specific security permissions must have been granted to manage collections	You must have the following security permissions to manage compliance settings: - To create and manage collections: **Create**, **Delete**, **Modify**, **Modify Folder**, **Move Object**, **Read** and **Read Resource** for the **Collection** Object. - To manage collection settings: **Modify Collection Setting** for the **Collection** Object. The **Modify Folder** permission is required for all collection folders, including the root folder.

Best practices for collections in System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the following best practices for collections in System Center Configuration Manager.

Do not use incremental updates for a large number of collections

When you enable the **Use incremental updates for this collection** option, this configuration might cause evaluation delays when you enable it for many collections. The threshold is about 200 collections in your hierarchy. The exact number depends on the following factors:

- The total number of collections
- The frequency of new resources being added and changed in the hierarchy
- The number of clients in your hierarchy
- The complexity of collection membership rules in your hierarchy

Make sure that maintenance windows are large enough to deploy critical software updates

You can configure maintenance windows for device collections to restrict the times that Configuration Manager can install software on these devices. If you configure the maintenance window to be too small, the client might not be able to install critical software updates, which leaves the client vulnerable to the attack that is mitigated by the software update.

How to create collections in Configuration Manager

8/15/2019 • 11 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Collections are groupings of users or devices. Use collections for tasks like managing applications, deploying compliance settings, or installing software updates. You can also use collections to manage groups of client settings or use them with role-based administration to specify the resources that an administrative user can access. Configuration Manager contains several built-in collections. For more information, see Introduction to collections.

> **NOTE**
> A collection can contain users or devices, but not both.

The information in this article can help you create collections in Configuration Manager. You can also import collections that were created at the current Configuration Manager site or at another one. For more information about how to export and import collections, see How to manage collections.

Collection rules

There are different types of rules that you can use to configure the members of a collection in Configuration Manager.

Direct rule

Use direct rules to choose the users or computers that you want to add to a collection. The membership doesn't change unless you remove a resource from Configuration Manager. Before you can add the resources to a direct rule collection, Configuration Manager must have discovered them or you must have imported them. Direct rule collections have more administrative overhead than query rule collections because they require manual changes.

Query rule

Dynamically update the membership of a collection based on a query that Configuration Manager runs on a schedule. For example, you can create a collection of users that are a member of the Human Resources organizational unit in Active Directory Domain Services. This collection is automatically updated when new users are added to or removed from the Human Resources organizational unit.

For example queries that you can use to build collections, see How to create queries.

Device category rule

You can make management of your devices easier by associating device categories with the device collections.

For more information, see Automatically categorize devices into collections.

Include collection rule

Include the members of another collection in a Configuration Manager collection. If the included collection changes, Configuration Manager updates the membership of the current collection on a schedule.

You can add multiple include collection rules to a collection.

Exclude collection rule

Exclude collection rules let you exclude the members of one collection from another Configuration Manager

collection. If the excluded collection changes, Configuration Manager updates the membership of the current collection on a schedule.

You can add multiple exclude collection rules to a collection. If a collection includes both include collection and exclude collection rules and there's a conflict, the exclude collection rule takes priority.

Example

You create a collection that has one include collection rule and one exclude collection rule. The include collection rule is for a collection of Dell desktops. The exclude collection is for a collection of computers that have less than 4 GB of RAM. The new collection contains Dell desktops that have at least 4 GB of RAM.

Create a collection

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace.

   - To create a *device collection*, select the **Device Collections** node. Then, on the **Home** tab of the ribbon, in the **Create** group, select **Create Device Collection**.

   - To create a *user collection*, select the **User Collections** node. Then, on the **Home** tab of the ribbon, in the **Create** group, select **Create User Collection**.

2. On the **General** page of the wizard, provide a **Name** and a **Comment**. In the **Limiting collection** section, select **Browse**, and then select a limiting collection. The collection you're creating will contain only members from the limiting collection.

3. On the **Membership Rules** page, in the **Add Rule** list, select the type of membership rule that you want to use for the collection. You can configure multiple rules for each collection. The configuration for each rule varies. For more information on configuring each rule, see the following sections of this article:

   - Direct rule
   - Query rule
   - Device category rule
   - Include collection rule
   - Exclude collection rule

4. Also on the **Membership Rules** page, review the following settings.

   - **Use incremental updates for this collection**: Select this option to periodically scan for and update only new or changed resources from the previous collection evaluation. This process is independent of a full collection evaluation. By default, incremental updates occur at 5-minute intervals.

> **IMPORTANT**
>
> Collections with query rules that use the following classes don't support incremental updates:
>
> - SMS_G_System_CollectedFile
> - SMS_G_System_LastSoftwareScan
> - SMS_G_System_AppClientState
> - SMS_G_System_DCMDeploymentState
> - SMS_G_System_DCMDeploymentErrorAssetDetails
> - SMS_G_System_DCMDeploymentCompliantAssetDetails
> - SMS_G_System_DCMDeploymentNonCompliantAssetDetails
> - SMS_G_User_DCMDeploymentCompliantAssetDetails (for collections of users only)
> - SMS_G_User_DCMDeploymentNonCompliantAssetDetails (for collections of users only)
> - SMS_G_System_SoftwareUsageData
> - SMS_G_System_CI_ComplianceState
> - SMS_G_System_EndpointProtectionStatus
> - SMS_GH_System_*
> - SMS_GEH_System_*

- **Schedule a full update on this collection**: Schedule a regular full evaluation of the collection membership.

  Starting in version 1810, these changes in collection evaluation behavior can improve site performance:

  - Previously, when you configured a schedule on a query-based collection, the site would continue to evaluate the query whether or not you enabled the collection setting to **Schedule a full update on this collection**. To fully disable the schedule, you had to change the schedule to **None**.

    Now the site clears the schedule when you disable this setting. To specify a schedule for collection evaluation, enable the option to **Schedule a full update on this collection**.

    When you update your site, for any existing collection on which you specified a schedule, the site enables the option to **Schedule a full update on this collection**. While this configuration might not be your intent, it was the actual behavior of the schedule before you updated the site. To stop the site evaluating a collection on a schedule, disable this option.

  - You can't disable the evaluation of built-in collections like **All Systems**, but now you can configure the schedule. This behavior allows you to customize this action at a time that meets your requirements.

    > **TIP**
    >
    > On built-in collections, only change the **Time** of the custom schedule. Don't change the **Recurrence pattern**. Future iterations might enforce a specific recurrence pattern.

5. Complete the wizard to create the new collection. The new collection is displayed in the **Device Collections** node of the **Assets and Compliance** workspace.

> **NOTE**
> You must refresh or reload the Configuration Manager console to see the collection members. They don't appear in the collection until after the first scheduled update. You can also manually select **Update Membership** for the collection. It might take a few minutes for a collection update to complete.

Configure a direct rule

1. On the **Search for Resources** page of the **Create Direct Membership Rule Wizard**, specify the following information.

   - **Resource class**: Select the type of resource you want to search for and add to the collection. For example:

     - **System Resource**: Search for inventory data returned from client computers.
     - **Unknown Computer**: Select from values returned by unknown computers.
     - **User Resource**: Search for user information collected by Configuration Manager.
     - **User Group Resource**: Search for user group information collected by Configuration Manager.
   - **Attribute name**: Select the attribute associated with the selected resource class that you want to search for. For example:

     - If you want to select computers by their NetBIOS name, select **System Resource** in the **Resource class** list and **NetBIOS name** in the **Attribute name** list.
     - If you want to select users by their organizational unit (OU) name, select **User Resource** in the **Resource class** list and **User OU Name** in the **Attribute name** list.
   - **Exclude resources marked as obsolete**: If a client computer is marked as obsolete, don't include this value in the search results.
   - **Exclude resources that do not have the Configuration Manager client installed**: These resources won't be displayed in the search results.
   - **Value**: Enter a value to search the selected attribute name. Use the percent character (%) as a wildcard. For example:

     - To search for computers that have a NetBIOS name beginning with "M", enter **M%** in this field.
     - To search for users in the Contoso OU, enter **Contoso** in this field.
2. On the **Select Resources** page, select the resources that you want to add to the collection in the **Resources** list, and then select **Next**.

Configure a query rule

In the **Query Rule Properties** dialog box, specify the following information.

- **Name**: Specify a unique name for the query.
- **Import Query Statement**: Opens the **Browse Query** dialog box. Select a Configuration Manager query to use as the query rule for the collection.
- **Resource class**: Select the type of resource you want to search for and add to the collection. Select a value from **System Resource** to search for inventory data returned from client computers or from **Unknown Computer** to select from values returned by unknown computers.
- **Edit Query Statement**: Opens the **Query Statement Properties** dialog box, where you can write a query to use as the rule for the collection. For more information about queries, see Introduction to queries.

Device category rule

The following actions are available in the **Select Device Categories** window.

- **Create**: Specify a name to create a new category.
- **Rename**: Rename the selected category.
- **Delete**: Select one or more categories, and use this action to remove them from the list.

For more information, see Automatically categorize devices into collections.

Configure an include collection rule

In the **Select Collections** dialog box, select the collections you want to include in the new collection, and then select **OK**.

Configure an exclude collection rule

In the **Select Collections** dialog box, select the collections you want to exclude from the new collection, and then select **OK**.

Import a collection

When you export a collection from a site, Configuration Manager saves it as a Managed Object Format (MOF) file. Use this procedure to import that file into your site database. To complete this procedure, you need **Create** permissions on the collections class.

> **IMPORTANT**
> - Make sure the file contains only collection data, is from a trusted source, and hasn't been tampered with.
> - Make sure the file was exported from a site running the same version of Configuration Manager that you're using.

For more information about exporting collections, see How to manage collections.

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace. Select either the **User Collections** or the **Device Collections** node.
2. On the **Home** tab of the ribbon, in the **Create** group, select **Import Collections**.
3. On the **General** page of the **Import Collections Wizard**, select **Next**.
4. On the **MOF File Name** page, select **Browse**. Browse to the MOF file that contains the collection information you want to import.
5. Complete the wizard to import the collection. The new collection is displayed in the **User Collections** or **Device Collections** node of the **Assets and Compliance** workspace. Refresh or reload the Configuration Manager console to see the collection members for the newly imported collection.

Synchronize collection membership results to Azure Active Directory groups

(Introduced as a pre-release feature starting in version 1906)

> **NOTE**
> Synchronization of collection memberships to an Azure Active Directory (Azure AD) group is a pre-release feature that was first introduced in version 1906. To enable it, see the Pre-release features article.

You can enable the synchronization of collection memberships to an Azure Active Directory (Azure AD) group. This synchronization allows you to use your existing on premises grouping rules in the cloud by creating Azure

AD group memberships based on collection membership results. You can synchronize device collections. Only devices with an Azure Active Directory record are reflected in the Azure AD Group. Both Hybrid Azure AD Joined and Azure Active Director joined devices are supported.

The Azure AD synchronization happens every five minutes. It's a one-way process, from Configuration Manager to Azure AD. Changes made in Azure AD aren't reflected in Configuration Manager collections, but aren't overwritten by Configuration Manager. For example, if the Configuration Manager collection has two devices, and the Azure AD group has three different devices, after synchronization the Azure AD group has five devices.

Prerequisites

- Cloud Management
- Azure Active Directory user discovery

Create a group and set the owner in Azure AD

1. Go to https://portal.azure.com.
2. Navigate to **Azure Active Directory** > **Groups** > **All groups**.
3. Click **New group** and type in a **Group name** and optionally **Group description**.
4. Make sure that **Membership type** is **Assigned**.
5. Select **Owners**, then add the identity that will create the synchronization relationship in Configuration Manager.
6. Click **Create** to finish creating the Azure AD group.

Enable collection synchronization for the Azure service

1. In the Configuration Manager console, go to **Administration** > **Overview** > **Cloud Services** > **Azure Services**.
2. Right-click on the Azure AD tenant where you created the group and select **Properties**.
3. In the **Collection Synchronization** tab, check the box for the **Enable Azure Directory Group Sync**.
4. Click **OK** to save the setting.

Enable the collection to synchronize

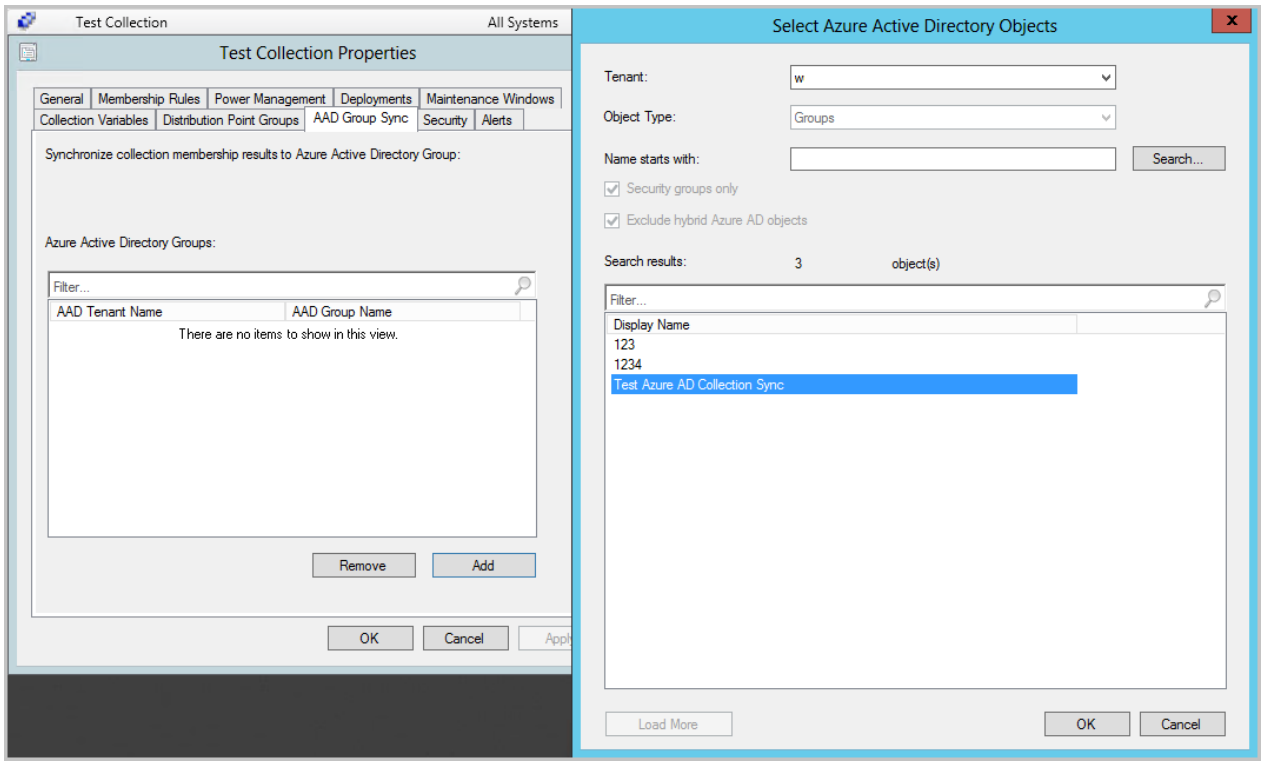
1. In the Configuration Manager console, go to **Assets and Compliance** > **Overview** > **Device Collections**.
2. Right-click on the collection to sync, then click **Properties**.
3. In the **AAD Group Sync** tab, click **Add**.
4. From the drop-down menu, select the **Tenant** where you created your Azure AD group.
5. Type in your search criteria in the **Name starts with** field, then click **Search**.

- If you are prompted to sign in, use the identity you specified as the owner for the Azure AD group.

1. Select the target group, then click **OK** to add the group and **OK** again to exit the collection's properties.
2. You'll need to wait about 5 to 7 minutes before you can verify the group memberships in the Azure portal.
   - To initiate a full synchronization, right-click the collection then select **Synchronize Membership**.

Verify the Azure AD group membership

1. Go to https://portal.azure.com.
2. Navigate to **Azure Active Directory** > **Groups** > **All groups**.
3. Find the group you created and select **Members**.
4. Confirm that the members reflect those in the Configuration Manager collection.
   - Only devices with Azure AD identity will show in the group.



Using PowerShell

You can use PowerShell to create and import collections. For more information, see:

- New-CMCollection
- Set-CMCollection
- Import-CMCollection

Next steps

Manage collections

How to manage collections in Configuration Manager

7/26/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the overview information in this article to help you perform management tasks for collections in Configuration Manager.

> **NOTE**
> For information about how to create Configuration Manager collections, see How to create collections.

How to manage device collections

In the **Assets and Compliance** workspace, select **Device Collections**, select the collection to manage, and then select a management task.

Show Members

Displays all of the resources that are members of the selected collection in a temporary node under the **Devices** node.

Add Selected Items

Provides the following options:

- **Add Selected Items to Existing Device Collection**: Opens the **Select Collection** dialog box. Select the collection to which you want to add the members of the selected collection. The selected collection is included in this collection by using an **Include Collections** membership rule.
- **Add Selected Items to New Device Collection**: Opens the **Create Device Collection Wizard** where you can create a new collection. The selected collection is included in this collection by using an **Include Collections** membership rule.

For more information, see How to create collections.

Install Client

Opens the **Install Client Wizard**. This wizard uses client push installation to install a Configuration Manager client on all computers in the selected collection. For more information, see Client push installation.

Run Script

Opens the **Run Script** wizard to run a PowerShell script on all of the clients in the collection. For more information, see Create and run PowerShell scripts.

Manage Affinity Requests

Opens the **Manage User Device Affinity Requests** dialog box. Approve or reject pending requests to establish user device affinities for devices in the selected collection. For more information, see Link users and devices with user device affinity

Clear Required PXE Deployments

Clears any required PXE boot deployments from all members of the selected collection. For more information, see Use PXE to deploy Windows over the network.

Update Membership

Evaluates the membership for the selected collection. For collections with many members, this update might take some time to finish. Use the **Refresh** action to update the display with the new collections members after the

update is completed.

Add Resources

Opens the **Add Resources to Collection** dialog box. Search for new resources to add to the selected collection. The icon for the selected collection displays an hourglass symbol while the update is in progress.

Client Notification

For more information, see Client notifications.

Endpoint Protection

For more information, see Client notifications.

Export

Opens the **Export Collection Wizard** that helps you export this collection to a Managed Object Format (MOF) file. This file can then be archived or imported at another Configuration Manager site. When you export a collection, referenced collections aren't exported. A referenced collection is referenced by the selected collection through the use of an **Include** or **Exclude** rule.

Copy

Creates a copy of the selected collection. The new collection uses the selected collection as a limiting collection.

Refresh

Refresh the view.

Delete

Deletes the selected collection. You can also delete all of the resources in the collection from the site database.

You can't delete the collections that are built into Configuration Manager. For a list of the built-in collections, see Introduction to collections.

Simulate Deployment

Opens the **Simulate Application Deployment Wizard**. This wizard lets you test the results of an application deployment without installing or uninstalling the application. For more information, see How to simulate application deployments.

Deploy

Displays the following options:

- **Application**: Opens the **Deploy Software Wizard**. Select and configure an application deployment to the selected collection. For more information, see How to deploy applications.
- **Program**: Opens the **Deploy Software Wizard**. Select and configure a package and program deployment to the selected collection. For more information, see Packages and programs.
- **Configuration Baseline**: Opens the **Deploy Configuration Baselines** dialog box. Configure the deployment of one or more configuration baselines to the selected collection. For more information, see How to deploy configuration baselines.
- **Task Sequence**: Opens the **Deploy Software Wizard**. Select and configure a task sequence deployment to the selected collection. For more information, see Manage task sequences to automate tasks.
- **Software Updates**: Opens the **Deploy Software Updates Wizard**. Configure the deployment of software updates to resources in the selected collection. For more information, see Manage software updates.

Clear Server Group Deployment Locks

Manually release all server group deployment locks for the collection. For more information, see Service a server group.

Move

Move the selected collection to another folder in the **Device Collections** node.

Properties

For more information, see Collection properties.

How to manage user collections

In the **Assets and Compliance** workspace, select **User Collections**, select the collection to manage, and then select a management task.

> **NOTE**
> The following actions are available on user collections, but the behaviors are the same as with device collections. Other than they apply to user collections and the users within. For more information, see the corresponding action under How to manage device collections.

- **Show Members**
- **Add Selected Items**
  - **Add Selected Items to Existing User Collection**
  - **Add Selected Items to New User Collection**
- **Manage Affinity Requests**
- **Update Membership**
- **Add Resources**
- **Export**
- **Copy**
- **Refresh**
- **Delete**
- **Simulate Deployment**
- **Deploy**
  - **Application**
  - **Program**
  - **Configuration Baseline**
- **Move**
- **Properties**

Collection properties

When you open the **Properties** dialog box for a collection, view and configure the following options:

General

View and configure general information about the selected collection including the collection name and the limiting collection.

Membership Rules

Configure the membership rules that define the membership of this collection. For more information, see How to create collections.

Power Management

Configure power management plans that you've assigned to computers in the selected collection. For more information, see Introduction to power management.

Deployments

Displays any software that you've deployed to members of the selected collection.

Maintenance Windows

View and configure maintenance windows that are applied to members of the selected collection. For more information, see How to use maintenance windows.

Collection Variables

Configure variables that apply to this collection and can be used by task sequences. For more information, see How to set task sequence variables.

Distribution Point Groups

Associate one or more distribution point groups to members of the selected collection. For more information, see Manage content and content infrastructure.

AAD Group Sync

Synchronize collection membership results to Azure Active Directory Groups. This synchronization is a pre-release feature starting in version 1906. For more information, see Create collections.

Security

Displays the administrative users who have permissions for the selected collection from associated roles and security scopes. For more information, see Fundamentals of role-based administration.

Alerts

Configure when alerts are generated for client status and Endpoint Protection. For more information, see How to configure client status and How to monitor Endpoint Protection.

Using PowerShell

PowerShell can be used to manage collections. For more information, see:

- Get-CMCollection
- Set-CMCollection
- New-CMCollection
- Copy-CMCollection
- Remove-CMCollection
- Import-CMCollection
- Export-CMCollection
- Get-CMCollectionMember
- Get-CMCollectionSetting
- Invoke-CMCollectionUpdate
- Add-CMCollectionMembershipRule
- Set-CMCollectionPowerManagement
- Get-CMCollectionMembershipRule
- Remove-CMCollectionMembershipRule
- Get-CMCollectionDirectMembershipRule
- Get-CMCollectionQueryMembershipRule
- Get-CMCollectionIncludeMembershipRule
- Add-CMCollectionToAdministrativeUser
- Remove-CMCollectionQueryMembershipRule
- Remove-CMCollectionDirectMembershipRule
- Get-CMCollectionExcludeMembershipRule
- Add-CMCollectionToDistributionPointGroup
- Remove-CMCollectionIncludeMembershipRule
- Remove-CMCollectionExcludeMembershipRule
- Remove-CMCollectionFromAdministrativeUser

How to use maintenance windows in System Center Configuration Manager

5/15/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Maintenance windows enable you to define a time when Configuration Manager operations can be carried out on a device collection. You use maintenance windows to help ensure that client configuration changes occur during periods that don't affect productivity. Starting in Configuration Manager version 1806, your users can see when their next maintenance window is from the **Installation status** tab in the **Software Center**.

The following operations support maintenance windows:

- Software deployments
- Software update deployments
- Compliance settings deployment and evaluation
- Operating system deployments
- Task sequence deployments

  Configure maintenance windows with a start date, a start and finish time, and a recurrence pattern. The maximum duration of a window has to be less than 24 hours. By default, computer restarts caused by a deployment aren't allowed outside of a maintenance window, but you can override the default. Maintenance windows affect only the time when the deployment program runs; applications configured to download and run locally can download content outside of the window.

  When a client computer is a member of a device collection that has a maintenance window, a deployment program runs only if the maximum allowed run time doesn't exceed the duration configured for the window. If the program fails to run, an alert is generated and the deployment is rerun during the next scheduled maintenance window that has available time.

Using multiple maintenance windows

When a client computer is a member of multiple device collections that have maintenance windows, these rules apply:

- If the maintenance windows don't overlap, they're treated as two independent maintenance windows.
- If the maintenance windows overlap, they're treated as a single maintenance window encompassing the time period covered by both maintenance windows. For example, if two windows, each an hour in duration overlap by 30 minutes, the effective duration of the maintenance window would be 90 minutes.

  When a user initiates an application installation from Software Center, the application is installed immediately, regardless of any maintenance windows.

  If an application deployment with a purpose of **Required** reaches its installation deadline during the nonbusiness hours configured by a user in Software Center, the application will be installed.

How to configure maintenance windows

1. In the Configuration Manager console, choose **Assets and Compliance**> **Device Collections**.

2. In the **Device Collections** list, select a collection. You can't create maintenance windows for the **All Systems** collection.
3. On the **Home** tab, in the **Properties** group, choose **Properties**.
4. In the **Maintenance Windows** tab of the **<collection name> Properties** dialog box, choose the **New** icon.
5. Complete the **<new> Schedule** dialog.
6. Make a selection from the **Apply this schedule to** drop-down list.
7. Choose **OK** and then close the **<collection name> Properties** dialog box.

Using PowerShell

PowerShell can be used to configure maintenance windows. For more information, see:

- Set-CMMaintenanceWindow
- Get-CMMaintenanceWindow
- New-CMMaintenanceWindow
- Remove-CMMaintenanceWindow

Automatically categorize devices into collections

5/23/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can create device categories, which can be used to automatically place devices in device collections when you are using Configuration Manager with Microsoft Intune. Users then have to choose a device category when they enroll a device in Intune. You can change a device category from the Configuration Manager console.

> **IMPORTANT**
> This capability works with the **June 2016** release of Microsoft Intune and later. Ensure that you have been updated to this release before you try out these procedures.

Create device categories

1. Go to **Assets and Compliance** > **Overview** > **Device Collections**.
2. On the **Home** tab, in the **Device Collections** group, choose **Manage Device Categories**.
3. Create, edit, or remove categories.

Associate a collection with a device category

When you associate a collection with a device category, all devices in that category will be added to the collection. You cannot add a device category rule to a built-in collection like **All Systems**.

1. On the **Membership Rules** tab of the **Properties** dialog box for a device collection, choose **Add Rule** > **Device Category Rule**.
2. In the **Select Device Categories** dialog box, select one or more device categories that will be applied to all devices in the collection.

Change the category of a device

1. In **Assets and Compliance** > **Overview** > **Devices**, select a device from the **Devices** list.
2. On the **Home** tab, in the **Device** group, choose **Change Category**.
3. Choose a category, then choose **OK**.

View which category a device belongs to

In **Assets and Compliance** > **Overview** > **Devices**, in the **Devices** list, the category is displayed in the **Device Category** column.

If the **Device Category** column is not displayed, right-click the heading of one of the columns in the **Devices** list (like **Name**), then select **Device Category**.

If you assign a device to a category, and subsequently delete the category, the report **List of Devices enrolled per user in Microsoft Intune** will display a GUID in the **Device Category** column, instead of a category name.

Security and privacy for collections in System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This topic contains security best practices and privacy information for collections in System Center Configuration Manager.

There is no privacy information specifically for collections in Configuration Manager. Collections are containers for resources, such as users and devices. Collection membership often depends on the information that Configuration Manager collects during standard operation. For example, by using resource information that has been collected from discovery or inventory, a collection can be configured to contain the devices that meet specified criteria. Collections might also be based on the current status information for client management operations, such as deploying software and checking for compliance. In addition to these query-based collections, administrative users can also add resources to collections.

For more information about collections, see Introduction to collections in System Center Configuration Manager. For more information about any security best practices and privacy information for Configuration Manager operations that can be used to configure collection membership, see Security best practices and privacy information for System Center Configuration Manager.

Security Best Practices for Collections

Use the following security best practice for collections.

SECURITY BEST PRACTICE	MORE INFORMATION
When you export or import a collection by using a Managed Object Format (MOF) file that is saved to a network location, secure the location, and secure the network channel.	Restricts who can access the network folder. Use Server Message Block (SMB) signing or Internet Protocol security (IPsec) between the network location and the site server to prevent an attacker from tampering with the exported collection data. Use IPsec to encrypt the data on the network to prevent information disclosure.

Security Issues for Collections

Collections have the following security issues:

- If you use collection variables, local administrators can read potentially sensitive information.

  Collection variables can be used when you deploy an operating system.

Introduction to hardware inventory in System Center Configuration Manager

7/3/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use hardware inventory in System Center Configuration Manager to collect information about the hardware configuration of client devices in your organization. To collect hardware inventory, you must select the **Enable hardware inventory on clients** setting in client settings.

After hardware inventory is enabled and the client runs a hardware inventory cycle, the client sends the information to a management point in the client's site. The management point then forwards the inventory information to the Configuration Manager site server, which stores the inventory information in the site database. Hardware inventory runs on clients according to the schedule that you specify in client settings.

View hardware inventory

You can use several methods to view the hardware inventory data that Configuration Manager collects, including these methods:

- Create queries that return devices that are based on a specific hardware configuration.
- Create query-based collections that are based on a specific hardware configuration. Query-based collection memberships automatically update on a schedule. You can use collections for several tasks, including software deployment.
- Run reports that display specific details about hardware configurations in your organization.
- Use Resource Explorer to view detailed information about the hardware inventory that's collected from client devices.

When hardware inventory runs on a client device, the first inventory data that the client returns is always a full inventory. Subsequent inventory data contains only delta inventory information. The site server processes delta inventory information in the order received. If delta information for a client is missing, the site server rejects additional delta information and directs the client to run a full inventory cycle.

Configuration Manager provides limited support for dual-boot computers. Configuration Manager can discover dual-boot computers but returns inventory information only from the operating system that's active when the inventory cycle runs.

> **NOTE**
>
> For information about how to use hardware inventory with clients that run Linux and UNIX, see Hardware inventory for Linux and UNIX in System Center Configuration Manager.

Extending Configuration Manager hardware inventory

In addition to the built-in hardware inventory in Configuration Manager, you can also use one of these methods to extend hardware inventory to collect more information:

- Enable, disable, add and remove inventory classes for hardware inventory from the Configuration Manager

console.

- Use NOIDMIF files to collect information about client devices that can't be inventoried by Configuration Manager. For example, you might want to collect device asset number information that exists only as a label on the device. NOIDMIF inventory is automatically associated with the client device that it was collected from.
- Use IDMIF files to collect information about assets that aren't associated with a Configuration Manager client, for example, projectors, photocopiers, and network printers.

Next steps

For more information about using these methods to extend Configuration Manager hardware inventory, see How to configure hardware inventory in System Center Configuration Manager.

How to extend hardware inventory in System Center Configuration Manager

5/9/2019 • 9 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Hardware inventory reads information from Windows PCs by using Windows Management Instrumentation (WMI). WMI is the Microsoft implementation of web-based Enterprise Management (WBEM), an industry standard for accessing management information in an enterprise. In previous versions of Configuration Manager, you extended hardware inventory by modifying the file sms_def.mof on the site server. This file contained a list of WMI classes that could be read by hardware inventory. Editing this file, you could enable and disable existing classes, and also create new classes to inventory.

The Configuration.mof file is used to define the data classes to be inventoried by hardware inventory on the client and is unchanged from Configuration Manager 2012. You can create data classes to inventory existing or custom WMI repository data classes or registry keys present on client systems.

The Configuration.mof file also defines and registers the WMI providers that access device information during hardware inventory. Registering providers defines the type of provider to be used and the classes that the provider supports.

When Configuration Manager clients request policy, the Configuration.mof is attached to the policy body. This file is then downloaded and compiled by clients. When you add, modify, or delete data classes from the Configuration.mof file, clients automatically compile these changes that are made to inventory-related data classes. No further action is necessary to inventory new or modified data classes on Configuration Manager clients. This file is located in **<CMInstallLocation>\Inboxes\clifiles.src\hinv** on primary site servers.

In Configuration Manager, you no longer edit the sms_def.mof file as you did in Configuration Manager 2007. Instead, you can enable and disable WMI classes, and add new classes to collect by hardware inventory by using client settings. Configuration Manager provides the following methods to extend hardware inventory.

> **NOTE**
> If you've manually changed the Configuration.mof file to add custom inventory classes, these changes will be overwritten when you update to version 1602. To keep using custom classes after you update, you must add them to the "Added extensions" section of the Configuration.mof file after you update to 1602.
> However, you must not modify anything above this section, as these sections are reserved for modification by Configuration Manager. A backup of your custom Configuration.mof can be found in:
> **<CM Install dir>\data\hinvarchive**.

METHOD	MORE INFORMATION
Enable or disable existing inventory classes	Enable or disable the default inventory classes or create custom client settings that allow you to collect different hardware inventory classes from specified collections of clients. See the To enable or disable existing inventory classes procedure in this article.

METHOD	MORE INFORMATION
Add a new inventory class	Add a new inventory class from the WMI namespace of another device. See the To add a new inventory class procedure in this article.
Import and export hardware inventory classes	Import and export Managed Object Format (MOF) files that contain inventory classes from the Configuration Manager console. See the To import hardware inventory classes and To export hardware inventory classes procedures in this article.
Create NOIDMIF Files	Use NOIDMIF files to collect information about client devices that cannot be inventoried by Configuration Manager. For example, you might want to collect device asset number information that exists only as a label on the device. NOIDMIF inventory is automatically associated with the client device that it was collected from. See To create NOIDMIF files in this article.
Create IDMIF Files	Use IDMIF files to collect information about assets in your organization that are not associated with a Configuration Manager client, for example, projectors, photocopiers and network printers. See To create IDMIF files in this article.

Procedures to extend hardware inventory

These procedures help you to configure the default client settings for hardware inventory and they apply to all the clients in your hierarchy. If you want these settings to apply to only some clients, create a custom client device setting and assign it to a collection of specific clients. See How to configure client settings in System Center Configuration Manager.

To enable or disable existing inventory classes

1. In the Configuration Manager console, choose **Administration** > **Client Settings** > **Default Client Settings**.
2. On the **Home** tab, in the **Properties** group, choose **Properties**.
3. In the **Default Client Settings** dialog box, choose **Hardware Inventory**.
4. In the **Device Settings** list, click **Set Classes**.
5. In the **Hardware Inventory Classes** dialog box, select or clear the classes and class properties to be collected by hardware inventory. You can expand classes to select or clear individual properties within that class. Use the **Search for inventory classes** field to search for individual classes.

> **IMPORTANT**
> When you add new classes to Configuration Manager hardware inventory, the size of the inventory file that is collected and sent to the site server will increase. This might negatively affect the performance of your network and Configuration Manager site. Enable only the inventory classes that you want to collect.

To add a new inventory class

You can only add inventory classes from the hierarchy's top level server by modifying the default client settings. This option is not available when you create custom device settings.

1. In the Configuration Manager console, choose **Administration** > **Client Settings** > **Default Client Settings**.

2. On the **Home** tab, in the **Properties** group, choose **Properties**.
3. In the **Default Client Settings** dialog box, choose **Hardware Inventory**.
4. In the **Device Settings** list, choose **Set Classes**.
5. In the **Hardware Inventory Classes** dialog box, choose **Add**.
6. In the **Add Hardware Inventory Class** dialog box, click **Connect**.
7. In the **Connect to Windows Management Instrumentation (WMI)** dialog box, specify the name of the computer from which you will retrieve the WMI classes and the WMI namespace to use for retrieving the classes. If you want to retrieve all classes below the WMI namespace that you specified, click **Recursive**. If the computer you are connecting to is not the local computer, supply login credentials for an account that has permission to access WMI on the remote computer.
8. Choose **Connect**.
9. In the **Add Hardware Inventory Class** dialog box, in the **Inventory classes** list, select the WMI classes that you want to add to Configuration Manager hardware inventory.
10. If you want to edit information about the selected WMI class, choose **Edit**, and in the **Class qualifiers** dialog box, provide the following information:

    - **Display name** - This name will be displayed in Resource Explorer.
    - **Properties** - Specify the units in which each property of the WMI class will be displayed.

      You can also designate properties as a key property to help uniquely identify each instance of the class. If no key is defined for the class and multiple instances of the class are reported from the client, only the latest instance that is found is stored in the database.

      When you've finished configuring the properties, click **OK** to close the **Class qualifiers** dialog box and the other open dialogs.

To import hardware inventory classes

You can only import inventory classes when you modify the default client settings. However, you can use custom client settings to import information that doesn't include a schema change, such as changing the property of an existing class from **True** to **False**.

1. In the Configuration Manager console, choose **Administration** > **Client Settings** > **Default Client Settings**.
2. On the **Home** tab, in the **Properties** group, choose **Properties**.
3. In the **Default Client Settings** dialog box, choose **Hardware Inventory**.
4. In the **Device Settings** list, choose **Set Classes**.
5. In the **Hardware Inventory Classes** dialog box, choose **Import**.
6. In the **Import** dialog box, select the Managed Object Format (MOF) file that you want to import, and then choose **OK**. Review the items that will be imported, and then click **Import**.

To export hardware inventory classes

1. In the Configuration Manager console, choose **Administration** > **Client Settings** > **Default Client Settings**.
2. On the **Home** tab, in the **Properties** group, choose **Properties**.
3. In the **Default Client Settings** dialog box, choose **Hardware Inventory**.

4. In the **Device Settings** list, choose **Set Classes**.
5. In the **Hardware Inventory Classes** dialog box, choose **Export**.

> **NOTE**
> When you export classes, all currently selected classes will be exported.

6. In the **Export** dialog box, specify the Managed Object Format (MOF) file that you want to export the classes to, and then choose **Save**.

Configure hardware inventory to collect strings larger than 255 characters

Beginning in Configuration Manager 1802, you can specify the length of strings to be greater than 255 characters for hardware inventory properties. This change applies only to newly added classes and for hardware inventory properties that aren't keys.

1. In the **Administration** workspace, click on **Client Settings** highlight a client device setting to edit, right-click then select **Properties**.
2. Select **Hardware Inventory**, then **Set Classes**, and **Add**.
3. Click the **Connect** button.
4. Fill in **Computer Name**, **WMI namespace**, select **recursive** if needed. Provide credentials if necessary to connect. Click **Connect** to view the namespace classes.
5. Select a new class then click **Edit**.
6. Change the **Length** of your property that is a string, other than the key, to be greater than 255. Click **OK**.
7. Ensure that the edited property is selected for **Add Hardware Inventory Class** and click **OK**.

How to Use Management Information Files (MIF Files) to extend hardware inventory

Use Management Information Format (MIF) files to extend hardware inventory information collected from clients by Configuration Manager. During hardware inventory, the information stored in MIF files is added to the client inventory report and stored in the site database, where you can use the data in the same ways that you use default client inventory data. There are two types of MIF files, NOIDMIF, and IDMIF.

> **IMPORTANT**
> Before you can add information from MIF files to the Configuration Manager database, you must create or import class information for them. For more information, see the sections To add a new inventory class and To import hardware inventory classes in this article.

To create NOIDMIF files

NOIDMIF files can be used to add information to a client hardware inventory that can't normally be collected by Configuration Manager and is associated with a particular client device. For example, many companies label each computer in the organization with an asset number and then catalog these numbers manually. When you create a NOIDMIF file, this information can be added to the Configuration Manager database and be used for queries and reporting. For information about creating NOIDMIF files, see the Configuration Manager SDK documentation.

IMPORTANT

When you create a NOIDMIF file, it must be saved in an ANSI encoded format. NOIDMIF files saved in UTF-8 encoded format cannot be read by Configuration Manager.

After you create a NOIDMIF file, store it in the *%Windir%***\CCM\Inventory\Noidmifs** folder on each client. Configuration Manager will collect information from NODMIF files in this folder during the next scheduled hardware inventory cycle.

To create IDMIF files

IDMIF files can be used to add information about assets that couldn't normally be inventoried by Configuration Manager and isn't associated with a particular client device, to the Configuration Manager database. For example, you could use IDMIFS to collect information about projectors, DVD players, photocopiers, or other equipment that doesn't have a Configuration Manager client. For information about creating IDMIF files, see the Configuration Manager SDK documentation.

After you create an IDMIF file, store it in the *%Windir%***\CCM\Inventory\Idmifs** folder on client computers. Configuration Manager will collect information from this file during the next scheduled hardware inventory cycle. You must declare new classes for information contained in the file by adding or importing them.

NOTE

MIF files could contain large amounts of data and collecting this data could negatively affect the performance of your site. Enable MIF collection only when required and configure the option **Maximum custom MIF file size (KB)** in the hardware inventory settings. For more information, see Introduction to hardware inventory in System Center Configuration Manager.

How to configure hardware inventory in System Center Configuration Manager

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This procedure configures the default client settings for hardware inventory and will apply to all the clients in your hierarchy. If you want these settings to apply to only some clients, create a custom device client setting and assign it to a collection that contains the devices that you want to use hardware inventory. See How to configure client settings in System Center Configuration Manager.

> **NOTE**
> If a client device receives hardware inventory settings from multiple sets of client settings, then the hardware inventory classes from each set of settings will be merged when the client reports hardware inventory. Additionally, not checking a class in a custom client setting with a higher priority doesn't disable the client from inventorying that class.

To disable a specific hardware inventory class on a majority of systems except a few, the class needs to be unchecked in the default client settings. Then create a custom client setting to enable the class, and deploy it to the target systems.

To configure hardware inventory

1. In the Configuration Manager console, choose **Administration** > **Client Settings** > **Default Client Settings**.
2. On the **Home** tab, in the **Properties** group, choose **Properties**.
3. In the **Default Settings** dialog box, choose **Hardware Inventory**.
4. In the **Device Settings** list, configure the following:
   - **Enable hardware inventory on clients** - Select **Yes**.
   - **Hardware inventory schedule** - Click **Schedule** to specify the interval at which clients collect hardware inventory.
5. Configure other hardware inventory client settings that you require.

Client devices will be configured with these settings when they next download client policy. To initiate policy retrieval for a single client, see How to manage clients in System Center Configuration Manager.

How to use Resource Explorer to view hardware inventory in Configuration Manager

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use Resource Explorer in Configuration Manager to view information about hardware inventory. The site collects this information from clients in your hierarchy.

> **TIP**
> Resource Explorer doesn't display any data until a hardware inventory cycle runs on the client to which you're connecting.

Overview

Resource Explorer has the following sections related to hardware inventory:

- **Hardware**: Shows the most recent hardware inventory collected from the specified client device.
  - The **Workstation Status** node shows the time and date of the last hardware inventory from the device.
- **Hardware History**: A history of inventoried items that changed since the last hardware inventory cycle.
  - Expand an item to see a **Current** node and one or more nodes with the historical date. Compare the information in the current node to one of the historical nodes to see the items that changed.

> **NOTE**
> By default, Configuration Manager deletes hardware inventory data that's been inactive for 90 days. Adjust this number of days in the **Delete Aged Inventory History** site maintenance task. For more information, see Maintenance tasks.

How to open Resource Explorer

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace, and select the **Devices** node. You can also select any collection in the **Device Collections** node.
2. Select a device. In the ribbon, on the **Home** tab and **Devices** group, click **Start**, and then select **Resource Explorer**.

> **TIP**
> In Resource Explorer, right-click an item in the right results pane for additional actions. Click **Properties** to view that item in a different format.

Use of large integer values

In Configuration Manager versions 1802 and prior, hardware inventory has a limit for integers larger than 4,294,967,296 (2^32). This limit can be reached for attributes such as hard drive sizes in bytes. The management point doesn't process integer values above this limit, so no value is stored in the database.

Starting in version 1806, the limit is increased to 18,446,744,073,709,551,616 (2^64).

For a property with a value that doesn't change, like total disk size, you may not immediately see the value after upgrading the site. Most hardware inventory is a delta report. The client only sends values that change. To work around this behavior, add another property to the same class. This action causes the client to update all properties in the class that changed.

See also

For information about how to view hardware inventory from clients that run Linux and UNIX, see How to monitor clients for Linux and UNIX servers.

Resource Explorer also shows Software Inventory. For more information, see How to use Resource Explorer to view software inventory.

Hardware inventory for Linux and UNIX in Configuration Manager

9/5/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

> **IMPORTANT**
>
> Starting in version 1902, Configuration Manager doesn't support Linux or UNIX clients.
>
> Consider Microsoft Azure Management for managing Linux servers. Azure solutions have extensive Linux support that in most cases exceed Configuration Manager functionality, including end-to-end patch management for Linux.

The Configuration Manager client for Linux and UNIX supports hardware inventory. After you collect hardware inventory you can run view inventory in the resource explorer or Configuration Manager reports, and use this information to create queries and collections that enable the following operations:

- Software deployment
- Enforce maintenance windows
- Deploy custom client settings

Hardware inventory for Linux and UNIX servers uses a standards-based Common Information Model (CIM) server. The CIM server runs as a software service (or daemon) and provides a management infrastructure that is based on Distributed Management Task Force (DMTF) standards. The CIM server provides functionality that is similar to the Windows Management Infrastructure (WMI) CIM capabilities that are available on Windows-based computers.

Beginning with cumulative update 1, the client for Linux and UNIX uses the open-source **omiserver** version 1.0.6 from the **Open Group**. (Prior to cumulative update 1, the client used **nanowbem** as its CIM server).

The CIM server installs as part of the client for Linux and UNIX. The client for Linux and UNIX communicates directly with the CIM server and doesn't use the WS-MAN interface of the CIM server. The WS-MAN port on the CIM server is disabled when the client installs. Microsoft developed the CIM server that is now available as open source through the Open Management Infrastructure (OMI) project. For more information about the Open Management Infrastructure project, see The Open Group website.

Hardware Inventory on Linux and UNIX servers operates by mapping existing Win32 WMI classes and properties to equivalent classes and properties for Linux and UNIX servers. This one-to-one mapping of classes and properties enables the Linux and UNIX hardware inventory to integrate with Configuration Manager. Inventory data from Linux and UNIX servers displays along with inventory from Windows-based computers in the Configuration Manager console and reports. This behavior provides a consistent heterogeneous management experience.

> **TIP**
>
> You can use the **Caption** value for the **Operating System** class to identify different Linux and UNIX operating systems in queries and collections.

Configuring hardware inventory for Linux and UNIX servers

You can use the default client settings or create custom client device settings to configure hardware inventory. When you use custom client device settings, you can configure the classes and properties you want to collect from only your Linux and UNIX servers. You can also specify custom schedules for when to collect full and delta inventories from your Linux and UNIX servers.

The client for Linux and UNIX supports the following hardware inventory classes that are available on Linux and UNIX servers:

- Win32_BIOS
- Win32_ComputerSystem
- Win32_DiskDrive
- Win32_DiskPartition
- Win32_NetworkAdapter
- Win32_NetworkAdapterConfiguration
- Win32_OperatingSystem
- Win32_Process
- Win32_Service
- Win32Reg_AddRemovePrograms
- SMS_LogicalDisk
- SMS_Processor

Not all properties for these inventory classes are enabled for Linux and UNIX computers in Configuration Manager.

Operations for hardware inventory

After you collect hardware inventory from your Linux and UNIX servers, you can view and use this information the same way you view inventory you collect from other computers:

- Use Resource Explorer to view detailed information about the hardware inventory from Linux and UNIX servers
- Create queries based on specific hardware configurations
- Create query-based collections that are based on specific hardware configurations
- Run reports that display specific details about hardware configurations

Hardware inventory on a Linux or UNIX server runs according to the schedule you configure in client settings. By default, this schedule is every seven days. The client for Linux and UNIX supports both full inventory cycles and delta inventory cycles.

You can also force the client on a Linux or UNIX server to immediately run hardware inventory. To run hardware inventory, on a client use **root** credentials to run the following command to start a hardware inventory cycle:

```
/opt/microsoft/configmgr/bin/ccmexec -rs hinv
```

Actions for hardware inventory are entered into the client log file, **scxcm.log**.

How to use Open Management Infrastructure to create custom hardware inventory

The client for Linux and UNIX supports custom hardware inventory that you can create by using the Open Management Infrastructure (OMI). To do so, you use the following steps:

1. Create a custom inventory provider by using the OMI source
2. Configure computers to use the new provider to report inventory
3. Enable Configuration Manager to support the new provider

Create a custom hardware inventory provider for Linux and UNIX computers:

To create a custom hardware inventory provider for the Configuration Manager client for Linux and UNIX, use **OMI Source - v.1.0.6** and follow the instructions from the OMI Getting Started Guide. This process includes creating a Managed Object Format (MOF) file that defines the schema of the new provider. Later, you import the MOF file to Configuration Manager to enable support of the new custom inventory class.

Both the OMI Source - v.1.0.6, and the OMI Getting Started Guide are available for download from The Open Group website. You can locate these downloads on the **Documents** tab at the following web page on the OpenGroup.org website: Open Management Infrastructure (OMI).

Configure each computer that runs Linux or UNIX with the custom hardware inventory provider:

After you create a custom inventory provider, you must copy and then register the provider library file on each computer that has inventory you want to collect.

1. Copy the provider library to each Linux and UNIX computer from which you want to collect inventory. The name of the provider library resembles the following name: **XYZ_MyProvider.so**
2. Next, on each Linux and UNIX computer, register the provider library with the OMI server. The OMI server installs on the computer when you install the Configuration Manager client for Linux and UNIX but you must manually register custom providers. Use the following command line to register the provider:
   `/opt/microsoft/omi/bin/omireg XYZ_MyProvider.so`
3. After you register the new provider, test the provider by using the **omicli** tool. The **omicli** tool is installed on each Linux and UNIX computer when you install the Configuration Manager client for Linux and UNIX. For example, where **XYZ_MyProvider** is the name of the provider you created, run the following command on the computer: **/opt/microsoft/omi/bin/omicli ei root/cimv2 XYZ_MyProvider**

   For information about **omicli** and testing custom providers, see the OMI Getting Started Guide.

> **TIP**
> Use software distribution to deploy custom providers and to register custom providers on each Linux and UNIX client computer.

Enable the new inventory class in Configuration Manager:

Before Configuration Manager can report on inventory that's reported by the new provider on Linux and UNIX computers, you must import the Managed Object Format (MOF) file that defines the schema of your custom provider.

To import a custom MOF file into Configuration Manager, see How to configure hardware inventory in System Center Configuration Manager.

Security and privacy for hardware inventory in System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This topic contains security and privacy information for hardware inventory in System Center Configuration Manager.

Security best practices for hardware inventory

Use the following security best practices for when you collect hardware inventory data from clients:

SECURITY BEST PRACTICE	MORE INFORMATION
Sign and encrypt inventory data	When clients communicate with management points by using HTTPS, all data that they send is encrypted by using SSL. However, when client computers use HTTP to communicate with management points on the intranet, client inventory data and collected files can be sent unsigned and unencrypted. Make sure that the site is configured to require signing and use encryption. In addition, if clients can support the SHA-256 algorithm, select the option to require SHA-256.
Do not collect IDMIF and NOIDMIF files in high-security environments	You can use IDMIF and NOIDMIF file collection to extend hardware inventory collection. When necessary, Configuration Manager creates new tables or modifies existing tables in the Configuration Manager database to accommodate the properties in IDMIF and NOIDMIF files. However, Configuration Manager does not validate IDMIF and NOIDMIF files, so these files could be used to alter tables that you do not want altered. Valid data could be overwritten by invalid data. In addition, large amounts of data could be added and the processing of this data might cause delays in all Configuration Manager functions. To mitigate these risks, configure the hardware inventory client setting **Collect MIF files** as **None**.

Security issues for hardware inventory

Collecting inventory exposes potential vulnerabilities. Attackers can perform the following:

- Send invalid data, which will be accepted by the management point even when the software inventory client setting is disabled and file collection is not enabled.
- Send excessively large amounts of data in a single file and in lots of files, which might cause a denial of service.
- Access inventory information as it is transferred to Configuration Manager.

  Because a user with local administrative privileges can send any information as inventory data, do not consider inventory data that is collected by Configuration Manager to be authoritative.

  Hardware inventory is enabled by default as a client setting.

Privacy information for hardware inventory

Hardware inventory allows you to retrieve any information that is stored in the registry and in WMI on Configuration Manager clients. Software inventory allows you to discover all files of a specified type or to collect any specified files from clients. Asset Intelligence enhances the inventory capabilities by extending hardware and software inventory and adding new license management functionality.

Hardware inventory is enabled by default as a client setting and the WMI information collected is determined by options that you select. Software inventory is enabled by default but files are not collected by default. Asset Intelligence data collection is automatically enabled, although you can select the hardware inventory reporting classes to enable.

Inventory information is not sent to Microsoft. Inventory information is stored in the Configuration Manager database. When clients use HTTPS to connect to management points, the inventory data that they send to the site is encrypted during the transfer. If clients use HTTP to connect to management points, you have the option to enable inventory encryption. The inventory data is not stored in encrypted format in the database. Information is retained in the database until it is deleted by the site maintenance tasks **Delete Aged Inventory History** or **Delete Aged Collected Files** every 90 days. You can configure the deletion interval.

Before you configure hardware inventory, software inventory, file collection, or Asset Intelligence data collection, consider your privacy requirements.

Introduction to software inventory in System Center Configuration Manager

7/3/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use software inventory to collect information about files on client devices. Software inventory can also collect files from client devices and store them on the site server. Software inventory is collected when you select the **Enable software inventory on clients** setting in client settings. You can also schedule the operation in client settings.

After you enable software inventory and the clients run a software inventory cycle, the client sends the information to a management point in the client's site. The management point then forwards the inventory information to the Configuration Manager site server, which stores the information in the site database.

There are a few ways to view software inventory data:

- Create queries that return devices with specified files.
- Create query-based collections that include devices with specified files.
- Run reports that provide details about files on devices.
- Use Resource Explorer to examine detailed information about the files that were inventoried and collected from client devices.

When software inventory runs on a client device, the first report is a full inventory. Subsequent reports contain only delta inventory information. The site server processes delta information in the order received. If delta information for a client is missing, the site server rejects further delta information and directs the client to run a full inventory.

Configuration Manager can discover dual-boot computers but only returns inventory information from the operating system that's active at the time of inventory.

Mobile devices: See Software inventory for mobile devices enrolled with Microsoft Intune for information about collecting inventory for apps installed on mobile devices.

How to configure software inventory in System Center Configuration Manager

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This procedure configures the default client settings for software inventory and applies to all the computers in your hierarchy. If you want to apply these settings to only some computers, create a custom device client setting and assign it to a collection. For more information about how to create custom device settings, see How to configure client settings in System Center Configuration Manager.

To configure software inventory

1. In the Configuration Manager console, choose **Administration** > **Client Settings Default Client Settings**.
2. On the **Home** tab, in the **Properties** group, choose **Properties**.
3. In the **Default Settings** dialog box, choose **Software Inventory**.
4. In the **Device Settings** list, configure the following values:
   - **Enable software inventory on clients** - From the drop-down list, select **True**.
   - **Schedule software inventory and file collection schedule** - Configures the interval at which clients collect software inventory and files.
5. Configure the client settings that you require. The Software inventory section of the About client settings in System Center Configuration Manager article has a list of the client settings.

   Client computers will be configured with these settings when they next download client policy. To initiate policy retrieval for a single client, see How to manage clients in System Center Configuration Manager.

   > **TIP**
   > Error code 80041006 in inventoryprovider.log means the WMI provider is out of memory. That is, the memory quota limit for a provider has been hit and inventory provider cannot continue. In this case, the inventory agent creates a report with 0 entries so no inventory items are reported.
   > A possible solution for this error would be to reduce the scope of the software inventory collection. In circumstances when the error occurs after limiting the inventory scope, increasing the MemoryPerHost property defined in the _ProviderHostQuotaConfiguration class can provide a solution.

To exclude folders from software inventory

1. Using Notepad.exe, create an empty file named **Skpswi.dat**.
2. Right-click the **Skpswi.dat** file and click **Properties**. In the file properties for the Skpswi.dat file, select the **Hidden** attribute.
3. Place the **Skpswi.dat** file at the root of each client hard drive or folder structure that you want to exclude from software inventory.

NOTE

Software inventory will not inventory the client drive again unless this file is deleted from the drive on the client computer.

How to use Resource Explorer to view software inventory in System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use Resource Explorer in System Center Configuration Manager to view information about software inventory that has been collected from computers in your hierarchy.

> **NOTE**
> Resource Explorer will not display any inventory data until a software inventory cycle has run on the client.

Resource Explorer provides the following software inventory information:

- **Software**:
  - **Collected Files** - Files that were collected during software inventory.
  - **File Details** - Files that were inventoried during software inventory that are not associated with a specific product or manufacturer.
  - **Last Software Scan** - Date and time of the last software inventory and file collection for the client computer.
  - **Product Details** - Software products that were inventoried by software inventory, grouped by manufacturer.

To run Resource Explorer from the Configuration Manager console

1. In the Configuration Manager console, choose **Assets and Compliance**
2. In the **Assets and Compliance** workspace, choose **Devices** or open any collection that displays devices.
3. Choose the computer containing the inventory that you want to view and then, in the **Home** tab > **Devices** group, choose **Start** > **Resource Explorer**.
4. You can right-click any item in the right-pane of the Resource Explorer window and choose **Properties** to view the collected inventory information in a more readable format.

Security and privacy for software inventory in System Center Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This topic contains security and privacy information for software inventory in System Center Configuration Manager.

Security best practices for software inventory

Use the following security best practices for when you collect software inventory data from clients:

SECURITY BEST PRACTICE	MORE INFORMATION
Sign and encrypt inventory data	When clients communicate with management points by using HTTPS, all data that they send is encrypted by using SSL. However, when client computers use HTTP to communicate with management points on the intranet, client inventory data and collected files can be sent unsigned and unencrypted. Make sure that the site is configured to require signing and use encryption. In addition, if clients can support the SHA-256 algorithm, select the option to require SHA-256.
Do not use file collection to collect critical files or sensitive information	Configuration Manager software inventory uses all the rights of the LocalSystem account, which has the ability to collect copies of critical system files, such as the registry or security account database. When these files are available at the site server, someone with the Read Resource rights or NTFS rights to the stored file location could analyze their contents and possibly discern important details about the client in order to be able to compromise its security.
Restrict local administrative rights on client computers	A user with local administrative rights can send invalid data as inventory information.

Security issues for software inventory

Collecting inventory exposes potential vulnerabilities. Attackers can perform the following:

- Send invalid data, which will be accepted by the management point even when the software inventory client setting is disabled and file collection is not enabled.
- Send excessively large amounts of data in a single file and in lots of files, which might cause a denial of service.
- Access inventory information as it is transferred to Configuration Manager.

  If users know that they can create a hidden file named **Skpswi.dat** and place it in the root of a client hard drive to exclude it from software inventory, you will not be able to collect software inventory data from that computer.

  Because a user with local administrative privileges can send any information as inventory data, do not consider inventory data that is collected by Configuration Manager to be authoritative.

Software inventory is enabled by default as a client setting.

Privacy information for software inventory

Hardware inventory allows you to retrieve any information that is stored in the registry and in WMI on Configuration Manager clients. Software inventory allows you to discover all files of a specified type or to collect any specified files from clients. Asset Intelligence enhances the inventory capabilities by extending hardware and software inventory and adding new license management functionality.

Hardware inventory is enabled by default as a client setting and the WMI information collected is determined by options that you select. Software inventory is enabled by default but files are not collected by default. Asset Intelligence data collection is automatically enabled, although you can select the hardware inventory reporting classes to enable.

Inventory information is not sent to Microsoft. Inventory information is stored in the Configuration Manager database. When clients use HTTPS to connect to management points, the inventory data that they send to the site is encrypted during the transfer. If clients use HTTP to connect to management points, you have the option to enable inventory encryption. The inventory data is not stored in encrypted format in the database. Information is retained in the database until it is deleted by the site maintenance tasks **Delete Aged Inventory History** or **Delete Aged Collected Files** every 90 days. You can configure the deletion interval.

Before you configure hardware inventory, software inventory, file collection, or Asset Intelligence data collection, consider your privacy requirements.

Introduction to asset intelligence in Configuration Manager

5/9/2019 • 15 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Inventory and manage software license usage throughout your enterprise by using the asset intelligence catalog. Asset intelligence adds hardware inventory classes to improve the breadth of information that Configuration Manager collects. This information includes the hardware and software titles used in your environment. Over 60 reports present this information in an easy-to-use format. Many of these reports link to more specific reports. Query for general information and drill down to more detailed information.

Add custom information to the asset intelligence catalog. For example, custom software categories, software families, software labels, and hardware requirements. To dynamically update the asset intelligence catalog with the most current information available, connect it to the Microsoft Cloud.

Use asset intelligence to help reconcile your enterprise software license usage. Import software license information into the Configuration Manager site database to view it against what software is being used.

Asset intelligence catalog

The asset intelligence catalog is a set of database tables stored in the site database. These tables include categorization and identification information for over 300,000 software titles and versions. They also help manage hardware requirements for specific software titles.

Asset intelligence provides software license information for software titles that are being used, both of Microsoft and of non-Microsoft software. A predefined set of hardware requirements for software titles is available in the asset intelligence catalog, and you can create new user-defined hardware requirement information to meet custom requirements. You can also customize information in the asset intelligence catalog, and you can upload software title information to the Microsoft cloud for categorization.

Asset intelligence catalog updates that include newly released software are available for download periodically to perform bulk catalog updates. It can also be dynamically updated by using the asset intelligence synchronization point.

Software categories

Asset intelligence software categories are used to widely categorize inventoried software titles and as high-level groupings of more specific software families. For example, a software category could be energy companies, and a software family within that software category could be oil and gas or hydroelectric. Many software categories are predefined in the asset intelligence catalog. You can create user-defined categories to additionally define inventoried software. The validation state for all predefined software categories is always **Validated**. Custom software category information added to the asset intelligence catalog is **User Defined**.

For more information about how to manage software categories, see Configuring asset intelligence.

> **NOTE**
> Predefined software category information stored in the asset intelligence catalog is read-only. You can't change or delete it. Administrative users can add, modify, or delete user-defined software categories.

Software families

Asset intelligence software families are used to define inventoried software titles within software categories. Many software families are predefined in the asset intelligence catalog. You can create user-defined categories to additionally define inventoried software. The validation state for all predefined software families is always **Validated**. Custom software family information added to the asset intelligence catalog is **User-Defined**.

For more information about how to manage software families, see Configuring asset intelligence.

> **NOTE**
> Predefined software family information is read-only and can't be changed. Administrative users can add, modify, or delete user-defined software families.

Software labels

Asset intelligence custom software labels let you create filters to group software titles and to view them in asset intelligence reports. Use software labels to create user-defined groups of software titles that share a common attribute. For example, you could create a software label called Shareware, associate it with inventoried shareware titles, and run a report to display all software titles with that label. There are no predefined labels. The validation state for software labels is always **User Defined**.

For more information about how to manage software labels, see Configuring asset intelligence.

Hardware requirements

Use the hardware requirements information to verify that computers meet the hardware requirements for software titles before they're targeted for software deployments. Manage hardware requirements for software titles in the **Assets and Compliance** workspace in the **Hardware Requirements** node under the **Asset Intelligence** node.

Many hardware requirements are predefined in the asset intelligence catalog. Create new user-defined hardware requirement information to meet custom requirements. The validation state for all predefined hardware requirements is always **Validated**. User-defined hardware requirements information added to the asset intelligence catalog is **User Defined**.

For more information about how to manage hardware requirements, see Configuring asset intelligence.

> **NOTE**
> The hardware requirements displayed in the Configuration Manager console are retrieved from the asset intelligence catalog. They aren't based on inventoried software title information from clients.
>
> Hardware requirement information isn't updated as part of the synchronization process with Microsoft.
>
> You can create user-defined hardware requirements for inventoried software that doesn't have associated hardware requirements.

By default, the following information is displayed for each listed hardware requirement:

- **Software Title**: The software title associated with the hardware requirement
- **Minimum CPU (MHz)**: The minimum processor speed in megahertz (MHz) required by the software title
- **Minimum RAM (KB)**: The minimum RAM in kilobytes (KB) required by the software title
- **Minimum Disk Space (KB)**: The minimum free hard disk space in KB required by the software title
- **Minimum Disk Size (KB)**: The minimum hard disk size in KB required by the software title
- **Validation State**: The validation state for the hardware requirement

Predefined hardware requirements stored in the asset intelligence catalog are read-only and can't be deleted.

Administrative users can add, modify, or delete user-defined hardware requirements for software titles that aren't stored in the asset intelligence catalog.

Inventoried software titles

To view inventoried software title information in the Configuration Manager console, go to the **Assets and Compliance** workspace, expand the **Asset Intelligence** node, and select the **Inventoried Software** node. The hardware inventory agent collects the inventoried software information from Configuration Manager clients based on the software titles stored in the asset intelligence catalog.

> **NOTE**
> The hardware inventory agent collects inventory based on the asset intelligence hardware inventory reporting classes that you enable. For more information about how to enable the reporting classes, see Configuring asset intelligence.

By default, the following information is displayed for each inventoried software title:

- **Name**: The name of the inventoried software title
- **Vendor**: The name of the vendor that developed the inventoried software title
- **Version**: The product version of the inventoried software title
- **Category**: The software category that's currently assigned to the inventoried software title
- **Family**: The software family that's currently assigned to the inventoried software title
- **Label** [**1**, **2**, and **3**]: The custom labels associated with the software title. Inventoried software titles can have up to three custom labels associated with them.
- **Count**: The number of Configuration Manager clients that have inventoried the software title
- **State**: The validation state for the inventoried software title

> **NOTE**
> You can change the categorization information for inventoried software only at the top-level site in your hierarchy. This information includes product name, vendor, software category, and software family. After you modify the categorization information for predefined software, the validation state for the software changes from **Validated** to **User Defined**.

Asset intelligence synchronization point

The asset intelligence synchronization point is a Configuration Manager site system role. It's used to connect to the Microsoft cloud on TCP port 443 to manage dynamic catalog information updates. Install this site role only on the top-level site of the hierarchy. Configure all asset intelligence catalog customization by using a Configuration Manager console connected to the top-level site.

While you configure all updates at the top-level site, catalog information is replicated to other sites in the hierarchy. The site role lets you request on-demand catalog synchronization with Microsoft, or schedule automatic catalog synchronization. In addition to downloading new catalog information, the asset intelligence synchronization point can upload custom software title information to Microsoft for categorization. Microsoft treats all uploaded software titles as public information. Make sure that your custom software titles don't include confidential or proprietary information.

After you submit an uncategorized software title, Microsoft doesn't review it until there are at least four categorization requests from customers for the same software title. Then Microsoft researchers identify, categorize,

and make the software title categorization information available to all customers who are using the online service. Software titles that represent the most requests for categorization receive the highest priority to categorize. Custom software and line-of-business applications are unlikely to receive a category. Don't send these software titles to Microsoft for categorization.

An asset intelligence synchronization point is required to connect to the Microsoft cloud. For information about how to install the role, see Configuring asset intelligence.

Asset intelligence home page

The **Asset Intelligence** node in the **Assets and Compliance** workspace is the home page for asset intelligence in Configuration Manager. This home page displays a summary dashboard view for asset intelligence catalog information.

> **NOTE**
> The **Asset Intelligence** home page doesn't automatically update while you're viewing it.

The **Asset Intelligence** home page includes the following sections:

- **Catalog Synchronization**: Information about whether asset intelligence is enabled and the current status of the asset intelligence synchronization point.

  > **NOTE**
  > The home page only displays this section when you install an asset intelligence synchronization point.

  The section also provides the following information:

  - Synchronization schedule
  - If you've imported a customer license statement
  - The last status update
  - The time for the next scheduled update
  - The number of changes after you installed the asset intelligence synchronization point

- **Inventoried Software Status**: The count and percentage of inventoried software, software categories, and software families that are identified by Microsoft, identified by an administrator, pending online identification, or unidentified and not pending. The information displayed in table format shows the count for each, and the information displayed in the chart shows the percentage for each.

Asset intelligence reports

The asset intelligence reports are located in the Configuration Manager console, in the **Monitoring** workspace, in the **Asset intelligence** folder under the **Reporting** node. The reports provide information about hardware, license management, and software. For more information about reports in Configuration Manager, see Reporting.

> **NOTE**
>
> The accuracy of the quantity of installed software titles and license information displayed in asset intelligence reports might vary from the actual number of software titles installed or licenses that are used in the environment. This variation is because of the complex dependencies and limitations involved in inventorying software license information for software titles that are installed in enterprise environments. Don't use asset intelligence reports as the sole source for determining purchased software license compliance.

Hardware reports

Asset intelligence hardware reports provide information about hardware assets in the organization. By using hardware inventory information such as speed, memory, and peripheral devices, asset intelligence hardware reports can present information about USB devices, about hardware that must be upgraded, and even about computers that aren't ready for a specific software upgrade.

> **NOTE**
>
> Some user data in asset intelligence hardware reports is collected from the Windows security event log. For better report accuracy, clear this log when you reassign a computer to a new user.

License management reports

Asset intelligence license management reports provide data about licenses that are being used. The **License Ledger** report lists installed Microsoft applications in a format congruent with a Microsoft License Statement (MLS). This format provides a convenient method of matching acquired licenses with used licenses. Other license management reports provide information about computers acting as servers that run the key management service (KMS) for Windows activation statistics.

> **IMPORTANT**
>
> Several of the asset intelligence license management reports present information about the function of KMS, a method of administering volume licensing. If you haven't implemented a KMS server, some reports might not return any data.

Software reports

Asset intelligence software reports provide information about software families, categories, and specific software titles that are installed on computers in the organization. The software reports present information such as browser helper objects and software that starts automatically. These reports can be used to identify adware, spyware, and other malware. You can also use them to identify software redundancy to help streamline software acquisition and support.

Software identification tag reports

Asset intelligence software identification tag reports provide information about software that includes a software identification tag compliant with ISO/IEC 19770-2. The software identification tags provide authoritative information used to identify installed software. When you enable the **SMS_SoftwareTag** hardware inventory reporting class, Configuration Manager collects information about the software with software identification tags.

The following reports provide information about the software:

- **Software 14A - Search for software identification tag enabled software**: The count of installed software with a software identification tag enabled
- **Software 14B - Computers with specific software identification tag enabled software installed**: All computers that have installed software with a specific software identification tag enabled
- **Software 14C - Installed software identification tag enabled software on a specific computer**: All

installed software with a specific software identification tag enabled on a specific computer

Reporting limitations

Asset intelligence reports can provide large amounts of information about installed software titles and acquired software licenses that are being used. Don't use this information as the only source for determining acquired software license compliance.

Example dependencies

The accuracy of the quantity displayed in the asset intelligence reports for installed software titles and license information can vary from the actual amounts currently used. This variation is caused by the complex dependencies involved in inventorying software license information for software titles in use in enterprise environments. The following examples show the dependencies involved in inventorying installed software in the enterprise by using asset intelligence that might affect the accuracy of asset intelligence reports:

- **Client hardware inventory dependencies**: Asset intelligence installed software reports are based on data collected from Configuration Manager clients by extending hardware inventory to enable asset intelligence reporting. Because of this dependency on hardware inventory reporting, asset intelligence reports reflect data only from clients that successfully complete hardware inventory processes with the required asset intelligence WMI reporting classes enabled. Because Configuration Manager clients perform hardware inventory processes on a schedule defined by the administrative user, a delay might occur in data reporting that affects the accuracy of asset intelligence reports.

  For example, an inventoried licensed software title might be uninstalled after the client finishes a successful hardware inventory cycle. Asset intelligence reports display the software title as installed until the client's next scheduled hardware inventory reporting cycle.

- **Software packaging dependencies**: Asset intelligence reports are based on installed software title data collected by using standard Configuration Manager client hardware inventory processes. Some software title data might not be collected correctly. Examples that could cause inaccurate asset intelligence reporting:

  - Software installations that don't comply with standard installation processes
  - Software installations that were changed before installation

Legal limitations

The information displayed in asset intelligence reports is subject to many limitations. The information displayed in them doesn't represent legal, accounting, or other professional advice. The information provided by asset intelligence reports is for information only. Don't use it as the only source of information for determining software license usage compliance.

The following limitations are examples of using asset intelligence that might affect the accuracy of the reports:

- **Microsoft license usage quantity limitations**:

  - The quantity of acquired Microsoft software licenses is based on information that administrators supply. Closely review it to make sure that the correct number of software licenses is provided.
  - The reported quantity of Microsoft software licenses includes information only about Microsoft software licenses acquired through volume licensing programs. It doesn't reflect information for software licenses acquired through retail, OEM, or other software license sales channels.
  - Software licenses acquired in the last 45 days might not be included in the quantity of Microsoft software licenses reported because of software reseller reporting requirements and schedules.
  - Software license transfers from company mergers or acquisitions might not be reflected in Microsoft software license quantities.
  - Nonstandard terms and conditions in a Microsoft Volume Licensing (MVLS) agreement might affect the number of software licenses reported. They might require additional review by a Microsoft

representative.

- **Installed software title quantity limitations**: Configuration Manager clients must successfully complete hardware inventory reporting cycles for the asset intelligence reports to accurately report the quantity of installed software titles. There might be a delay between the installation or uninstallation of a licensed software title after a successful hardware inventory reporting cycle. This action may not be reflected in asset intelligence reports run before the client reports its next scheduled hardware inventory.
- **License reconciliation limitations**: The reconciliation of the quantity of installed software titles to the quantity of acquired software licenses is calculated by using a comparison of the license quantity specified by the administrator and the quantity of installed software titles collected from Configuration Manager client hardware inventories based on the schedule set by the administrator. This comparison doesn't represent a final Microsoft conclusion of the license positions. The actual license position depends on the specific software title license and usage rights granted by the license terms.

Asset intelligence validation states

Asset intelligence validation states represent the source and current validation status of asset intelligence catalog information. The following table shows possible asset intelligence validation states and administrator actions that can cause them.

STATE	DEFINITION	ADMINISTRATOR ACTION	COMMENT
Validated	Microsoft researchers defined the catalog item	None	Best state
User Defined	Microsoft researchers haven't defined the catalog item	Customize the local catalog information	This state is displayed in asset intelligence reports
Pending	Microsoft researchers haven't defined the catalog item, but you submitted the item to Microsoft for categorization	No further action after requesting categorization	Catalog item remains in this state until Microsoft researchers categorize the item, and you synchronize your asset intelligence catalog
Updateable	A user-defined catalog item has been categorized differently by Microsoft during catalog synchronization.	Use the **Resolve Conflict** action to decide whether to use the new categorization information or the previous user-defined value. For more information about how to resolve conflicts, see Operations for asset intelligence.	After you resolve a categorization conflict, the item isn't validated as conflicting again unless later categorization updates introduce new information about the item.
Uncategorized	Catalog item hasn't been defined by Microsoft researchers, the item hasn't been submitted to Microsoft for categorization, and the administrator hasn't assigned a user-defined categorization value.	Request categorization or customize your local catalog information. For more information, see Operations for asset intelligence.	None

NOTE

Catalog items that you submit to Microsoft for categorization have a validation state of **Pending** on a central administration site, but continue to be displayed with a validation state of **Uncategorized** on child primary sites.

For examples of when a validation state might transition from one state to another, see Example validation state transitions for asset intelligence.

Prerequisites for Asset Intelligence in System Center Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Asset Intelligence in System Center Configuration Manager has external dependencies and dependencies within the product.

Dependencies external to Configuration Manager

The following table provides the dependencies for Asset Intelligence that are external to Configuration Manager.

DEPENDENCY	MORE INFORMATION
Auditing of Success Logon Events Prerequisites	Four Asset Intelligence reports display information gathered from the Windows Security event logs on client computers. If the Security event log settings are not configured to log all Success logon events, these reports contain no data even if the appropriate hardware inventory reporting class is enabled. The following Asset Intelligence reports depend on collected Windows Security event log information: - Hardware 03A - Primary Computer Users - Hardware 03B - Computers for a Specific Primary Console User - Hardware 04A - Shared (Multi-user) Computers - Hardware 05A - Console Users on a Specific Computer To enable the Hardware Inventory Client Agent to inventory the information required to support these reports, you must first modify the Windows Security event log settings on clients to log all Success logon events, and enable the **SMS_SystemConsoleUser** hardware inventory reporting class. For more information about modifying Security event log settings to log all Success logon events, see Enable auditing of success logon events.

NOTE

The **SMS_SystemConsoleUser** hardware inventory reporting class retains successful logon event data for only the previous 90 days of the Security event log, regardless of the length of the log. If the Security event log has fewer than 90 days of data, the entire log is read.

Dependencies Internal to Configuration Manager

The following table provides the dependencies for Asset Intelligence that are internal to Configuration Manager.

DEPENDENCY	MORE INFORMATION

DEPENDENCY	MORE INFORMATION
Client Agent Prerequisites	The Asset Intelligence reports depend on client information that is obtained through client hardware and software inventory reports. To obtain the information necessary for all Asset Intelligence reports, the following client agents must be enabled: - Hardware Inventory Client Agent - Software Metering Client Agent
Hardware Inventory Client Agent Dependencies	To collect inventory data required for some Asset Intelligence reports, the Hardware Inventory Client Agent must be enabled. In addition, some hardware inventory reporting classes that Asset Intelligence reports depend on must be enabled on primary site server computers. For information about enabling the Hardware Inventory Client Agent, see How to extend hardware inventory in System Center Configuration Manager.
Software Metering Client Agent Dependencies	A number of Asset Intelligence software reports depend on the Software Metering Client Agent for data. For information about enabling the Software Metering Client Agent, see Monitor app usage with software metering in System Center Configuration Manager. The following Asset Intelligence reports depend on the Software Metering Client Agent to provide data: - Software 07A - Recently Used Executables by Number of Computers - Software 07B - Computers that Recently Used a Specified Executable - Software 07C - Recently Used Executables on a Specific Computer - Software 08A - Recently Used Executables by Number of Users - Software 08B - Users that Recently Used a Specified Executable - Software 08C - Recently Used Executables by a Specified User

DEPENDENCY	MORE INFORMATION
Asset Intelligence Hardware Inventory Reporting Class Prerequisites	Asset Intelligence reports in Configuration Manager depend on specific hardware inventory reporting classes. Until the hardware inventory reporting classes are enabled and clients have reported hardware inventory based on these classes, the associated Asset Intelligence reports do not contain any data. You can enable the following hardware inventory reporting classes to support Asset Intelligence reporting requirements: - SMS_SystemConsoleUsage[1] - SMS_SystemConsoleUser[1] - SMS_InstalledSoftware - SMS_AutoStartSoftware - SMS_BrowserHelperObject - Win32_USBDevice - SMS_InstalledExecutable - SMS_SoftwareShortcut - SoftwareLicensingService - SoftwareLicensingProduct - SMS_SoftwareTag [1] By default, the **SMS_SystemConsoleUsage** and **SMS_SystemConsoleUser** Asset Intelligence hardware inventory reporting classes are enabled. You can edit the Asset Intelligence hardware inventory reporting classes in the Configuration Manager console, in the **Assets and Compliance** workspace, when you click the **Asset Intelligence** node. For more information, see the Enable Asset Intelligence hardware inventory reporting classes section in the Configuring Asset Intelligence in System Center Configuration Manager topic.
Reporting services point	The reporting services point site system role must be installed before software updates reports can be displayed. For more information about creating a reporting services point, see Configuring Reporting in Configuration Manager.

Configure Asset Intelligence in System Center Configuration Manager

9/11/2019 • 12 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Asset Intelligence inventories and manages software license usage.

Steps to configure Asset Intelligence

- **Step 1**:To collect the inventory data required for Asset Intelligence reports, you have to enable the hardware inventory client agent as described in How to extend hardware inventory in System Center Configuration Manager.
- **Step 2**: Enable Asset Intelligence Hardware Inventory Reporting Classes.
- **Step 3**: Install an Asset Intelligence Synchronization Point
- **Step 4**: Enable auditing of success logon events
- **Step 5**: Import Software License Information
- **Step 6**: Configure Asset Intelligence maintenance tasks

Enable Asset Intelligence hardware inventory reporting classes

To enable Asset Intelligence in Configuration Manager sites, you must enable one or more Asset Intelligence hardware inventory reporting classes. You can enable the classes on the **Asset Intelligence** home page, or, in the **Administration** workspace, in the **Client Settings** node, in client settings properties. Use one of the following procedures.

To enable Asset Intelligence hardware inventory reporting classes from the Asset Intelligence home page

1. In the Configuration Manager console, choose **Asset and Compliance** > **Asset Intelligence**.
2. On the **Home** tab, in the **Asset Intelligence** group, choose **Edit Inventory Classes**.
3. To enable Asset Intelligence reporting, select **Enable all Asset Intelligence reporting classes** or **Enable only the selected Asset Intelligence reporting classes**, and select at least one reporting class from the classes displayed.

> **NOTE**
> Asset Intelligence reports that depend on the hardware inventory classes that you enable by using this procedure do not display data until clients have scanned for and returned hardware inventory.

To enable Asset Intelligence hardware inventory reporting classes from client settings properties

1. In the Configuration Manager console, choose **Administration** > **Client Settings** > **Default Client Agent Settings**. If you have created custom client settings, you can select those instead.
2. On the **Home** tab > **Properties** group, choose **Properties**.
3. Choose **Hardware Inventory** > **Set Classes**. .
4. Choose **Filter by category** > **Asset Intelligence Reporting Classes**. The list of classes is refreshed with only the Asset Intelligence hardware inventory reporting classes.
5. Select at least one reporting class from the list.

> **NOTE**
> Asset Intelligence reports that depend on the hardware inventory classes that you enable by using this procedure do not display data until clients have scanned for and returned hardware inventory.

Install an Asset Intelligence Synchronization Point

The Asset Intelligence synchronization point site system role is used to connect Configuration Manager sites to System Center Online to synchronize Asset Intelligence catalog information. The Asset Intelligence synchronization point can only be installed on a site system located at the top-level site of the Configuration Manager hierarchy and requires Internet access to synchronize with System Center Online by using TCP port 443.

In addition to downloading new Asset Intelligence catalog information, the Asset Intelligence synchronization point can upload custom software title information to System Center Online for categorization. Microsoft treats all uploaded software titles as public information. Ensure that your custom software titles do not contain confidential or proprietary information. For more information about requesting software title categorization, see Request a catalog update for uncategorized software titles.

To install an Asset Intelligence synchronization point site system role

1. In the Configuration Manager console, choose **Administration** > **Site Configuration** > **Servers and Site System Roles**.
2. Add the Asset Intelligence synchronization point site system role to a new or existing site system server:
   - For a **New site system server**: On the **Home** tab, in the **Create** group, choose **Create Site System Server** to start the wizard.

     > **NOTE**
     > By default, when Configuration Manager installs a site system role, the installation files are installed on the first available NTFS-formatted hard disk drive that has the most available free hard disk space. To prevent Configuration Manager from installing on specific drives, create an empty file named No_sms_on_drive.sms and copy it to the root folder of the drive before you install the site system server.

   - For an **Existing site system server**: Choose the server on which you want to install the Asset Intelligence synchronization point site system role. When you choose a server, a list of the site system roles that are already installed on the server are displayed in the details pane.

     On the **Home** tab, in the **Server** group, choose **Add Site System Role** to start the wizard.
3. Complete the **General** page. When you add the Asset Intelligence synchronization point to an existing site system server, verify the values that were previously configured.
4. On the **System Role Selection** page, select **Asset Intelligence Synchronization Point** from the list of available roles.
5. On the **Asset Intelligence Synchronization Point Connection Settings** page, choose **Next**.

   By default, the **Use this Asset Intelligence Synchronization Point** setting is selected and cannot be configured on this page. System Center Online accepts network traffic only over TCP port 443, therefore the **SSL port number** setting cannot be configured on this page of the wizard.
6. Optionally, you can specify a path to the System Center Online authentication certificate (.pfx) file. Typically, you do not specify a path for the certificate because the connection certificate is automatically provisioned during site role installation.
7. On the **Proxy Server Settings** page, specify whether the Asset Intelligence synchronization point will use a proxy server when connecting to System Center Online to synchronize the catalog and whether to use

credentials to connect to the proxy server.

> **WARNING**
> If a proxy server is required to connect to System Center Online, the connection certificate might also be deleted if the user account password expires for the account configured for proxy server authentication.

8. On the **Synchronization Schedule** page, specify whether to synchronize the Asset Intelligence catalog on a schedule. When you enable the synchronization schedule, you specify a simple or custom synchronization schedule. During scheduled synchronization, the Asset Intelligence synchronization point connects to System Center Online to retrieve the latest Asset Intelligence catalog. You can manually synchronize the Asset Intelligence catalog from the Asset Intelligence node in the Configuration Manager console. For the steps to manually synchronize the Asset Intelligence catalog, see the To manually synchronize the Asset Intelligence catalog section in the Operations for Asset Intelligence in System Center Configuration Manager.

9. Complete the wizard

Enable auditing of success logon events

Four Asset Intelligence reports display information gathered from the Windows Security event logs on client computers. Here's how to configure computer security policy logon settings to enable auditing of Success logon events.

To enable success logon event logging by using a local security policy

1. On a Configuration Manager client computer, choose **Start** > **Administrative Tools** > **Local Security Policy**.

2. In the **Local Security Policy** dialog box, under **Security Settings**, expand **Local Policies**, and then choose **Audit Policy**.

3. In the results pane, double-click **Audit logon events**, ensure that the **Success** check box is selected, and then choose **OK**.

To enable success logon event logging by using an Active Directory domain security policy

1. On a domain controller computer, choose **Start**, point to **Administrative Tools**, and then choose **Domain Security Policy**.

2. In the **Local Security Policy** dialog box, under **Security Settings**, expand **Local Policies**, and then choose **Audit Policy**.

3. In the results pane, double-click **Audit logon events**, ensure that the **Success** check box is selected, and then choose **OK**.

Import software license information

The following sections describe the procedures necessary to import both Microsoft and general software licensing information into the Configuration Manager site database by using the Import Software License Wizard. When you import software license information into the site database from license statement files, the site server computer account requires **Full Control** permissions for the NTFS file system to the file share that is used to import software license information.

> **IMPORTANT**
> When software license information is imported into the site database, existing software license information is overwritten. Ensure that the software license information file that you use with the Import Software License Wizard contains a complete listing of all necessary software license information.

To import software license information into the Asset Intelligence catalog

1. In the **Asset and Compliance** workspace, choose **Asset Intelligence**.
2. On the **Home** tab, in the **Asset Intelligence** group, choose **Import Software Licenses**.
3. On the **Import** page, specify whether you are importing a Microsoft Volume Licensing (MVLS) file (.xml or .csv) or a General License Statement file (.csv). For more information about creating a General License Statement file, see Create a general license statement information file for import later in this topic.

   > **WARNING**
   > To download an MVLS file in .csv format that you can import to the Asset Intelligence catalog, see Microsoft Volume Licensing Service Center. To access this information, you must have a registered account on the website. You must contact your Microsoft account representative for information about how to get your MVLS file in .xml format.

4. Enter the UNC path to the license statement file or choose **Browse** to select a network shared folder and file.

   > **NOTE**
   > The shared folder should be correctly secured to prevent unauthorized access to the licensing information file, and the computer account of the computer that the wizard is being run on must have Full Control permissions to the share that contains the license import file.

5. Complete the wizard.

Create a general license statement information file for import

A general license statement can also be imported into the Asset Intelligence catalog by using a manually created license import file in comma delimited (.csv) file format.

> **NOTE**
> While only the **Name**, **Publisher**, **Version**, and **EffectiveQuantity** fields are required to contain data, all fields must be entered on the first row of the license import file. All date fields should be displayed in the following format: Month/Day/Year, for example, 08/04/2008.

Asset Intelligence matches the products that you specify in the general license statement by using the product name and product version, but not publisher name. You must use a product name in the general license statement that is an exact match with the product name stored in the site database. Asset Intelligence takes the **EffectiveQuantity** number given in the general license statement and compares the number with the number of installed products found in Configuration Manager inventory.

> **TIP**
> To get a complete list of the product names stored in the Configuration Manager site database, you can run the following query on the site database: SELECT ProductName0 FROM v_GS_INSTALLED_SOFTWARE.

You can specify exact versions for a product or specify part of the version, such as only the major version. The following examples provide the resulting version matches for a general license statement version entry for a specific product.

GENERAL LICENSE STATEMENT ENTRY	MATCHING SITE DATABASE ENTRIES
Name: "MySoftware", ProductVersion0:"2"	ProductName0: "Mysoftware", ProductVersion0: "2.01.1234" ProductName0: "MySoftware", ProductVersion0: "2.02.5678" ProductName0: "MySoftware", ProductVersion0: "2.05.1234" ProductName0: "MySoftware", ProductVersion0: "2.05.5678" ProductName0: "MySoftware", ProductVersion0: "2.05.3579.000" ProductName0: "MySoftware", ProductVersion0: "2.10.1234"
Name: "MySoftware", Version "2.05"	ProductName0: "MySoftware", ProductVersion0: "2.05.1234" ProductName0: "MySoftware", ProductVersion0: "2.05.5678" ProductName0: "MySoftware", ProductVersion0: "2.05.3579.000"
Name: "Mysoftware", Version "2" Name: "Mysoftware", Version "2.05"	Error during import. The import fails when more than one entry matches the same product version.

To create a general license statement import file by using Microsoft Excel

1. Open Microsoft Excel and create a new spreadsheet.
2. On the first row of the new spreadsheet, enter all software license data field names.
3. On the second and subsequent rows of the new spreadsheet, enter software license information as required. Ensure that at least all of the required software license data fields are entered on subsequent rows for each software license to be imported. The software title name entered in the spreadsheet must be the same as the software title that is displayed in Resource Explorer for a client computer after hardware inventory has run.
4. Save the file in .csv format.
5. Copy the .csv file to the file share that is used to import software license information into the Asset Intelligence catalog.
6. In the Configuration Manager console, use the Import Software License Wizard to import the newly created .csv file.
7. Run the Asset Intelligence **License 15A - Third Party Software Reconciliation Report** to verify that the licensing information has been successfully imported into the Asset Intelligence catalog.

> **NOTE**
> For an example of a general software license file that you can use for testing purposes, see Example Asset Intelligence general license import file in System Center Configuration Manager.

Sample table to describe software licenses

When creating a general license statement import file, the information in the following table can be used to describe software licenses to be imported into the Asset Intelligence catalog.

COLUMN NAME	DATA TYPE	REQUIRED	EXAMPLE
Name	Up to 255 characters	Yes	Software title
Publisher	Up to 255 characters	Yes	Software publisher
Version	Up to 255 characters	Yes	Software title version
Language	Up to 255 characters	Yes	Software title language
EffectiveQuantity	Integer value	Yes	Number of licenses purchased
PONumber	Up to 255 characters	No	Purchase order information
ResellerName	Up to 255 characters	No	Reseller information
DateOfPurchase	Date value in the following format: MM/DD/YYYY	No	Date of license purchase
SupportPurchased	Bit value	No	0 or 1: Enter 0 for Yes, or 1 for No
SupportExpirationDate	Date value in the following format: MM/DD/YYYY	No	End date of purchased support
Comments	Up to 255 characters	No	Optional comments

Configure Asset Intelligence maintenance tasks

The following maintenance tasks are available for Asset Intelligence:

- **Check Application Title with Inventory Information**: Checks that the software title that is reported in software inventory is reconciled with the software title in the Asset Intelligence catalog. By default, this task is enabled and scheduled to run on Saturday after 12:00 A.M. and before 5:00 A.M. This maintenance task is only available at the top-level site in your Configuration Manager hierarchy.
- **Summarize Installed Software Data**: Provides the information that is displayed in the **Assets and Compliance** workspace, in the **Inventoried Software** node, under the **Asset Intelligence** node. When the task runs, Configuration Manager gathers a count for all inventoried software titles at the primary site. By default, this task is enabled and scheduled to run every day after 12:00 A.M. and before 5:00 A.M. This maintenance task is available only on primary sites.

To configure Asset Intelligence maintenance tasks

1. In the Configuration Manager console, choose **Administration** > **Site Configuration** > **Sites**.
2. Select the site on which to configure the Asset Intelligence maintenance task.
3. On the **Home** tab, in the **Settings** group, choose **Site Maintenance**. Select a task, and choose **Edit** to modify the settings.

   We recommend that you set the time period to off-peak hours of the site. The time period is the time interval in which the task can run. It is defined by the **Start after** and **Latest start time** specified in the **Task Properties** dialog box.

   You can initiate the task right away by selecting the current day and setting the **Start after** time to a couple minutes after the present time.

4. Choose **OK** to save your settings. The task now runs according to its schedule.

> **NOTE**
>
> If a task fails to run on the first attempt, Configuration Manager attempts to rerun the task until either the task runs successfully or until the time period in which the task can run has passed.

How to use Asset Intelligence in System Center Configuration Manager

8/30/2019 • 15 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This topic contains information to help you manage typical Asset Intelligence tasks in your System Center Configuration Manager hierarchy:

View Asset Intelligence information

You can view Asset Intelligence information on the **Asset Intelligence** home page and in Asset Intelligence reports.

Asset Intelligence home page

The **Asset Intelligence** home page displays a summary dashboard for Asset Intelligence catalog information. On the home page, you can view information about catalog synchronization and inventoried software status. The **Asset Intelligence** home page is divided into the following sections:

- **Catalog Synchronization**: Provides information about whether Asset Intelligence is enabled, the current status of the Asset Intelligence synchronization point, the synchronization schedule, whether the customer license statement is imported, when status was last updated and the time for the next scheduled update, and the number of changes that occurred after the Asset Intelligence synchronization point site system was installed.

  > **NOTE**
  > The Asset Intelligence catalog synchronization section of the **Asset Intelligence** home page is only displayed if an Asset Intelligence synchronization point site system role has been installed.

- **Inventoried Software Status**: Provides the count and percentage of inventoried software, software categories, and software families that are identified by Microsoft, identified by an administrative user, pending online identification, or unidentified and not pending. The information displayed in table format shows the count for each, while the information displayed in the chart shows the percentage for each.

  Use the following procedure to view Asset Intelligence information on the **Asset Intelligence** home page.

To view Asset Intelligence information on the Asset Intelligence home page

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Asset and Compliance** workspace, click **Asset Intelligence**. The Asset Intelligence reports are displayed.

Asset Intelligence reports

There are over 60 Asset Intelligence reports that display the information collected by Asset Intelligence. Many of these reports link to more specific reports in which you can query for general information and drill down to more detailed information. The Asset Intelligence reports are located in the Configuration Manager console, in the **Monitoring** workspace, under the **Reporting** node. The reports provide information about hardware, license management, and software. For more information about reports in Configuration Manager, see Reporting in System Center Configuration Manager.

> **NOTE**
>
> The accuracy of installed software title quantities and license information displayed in Asset Intelligence reports might vary from the actual number of software titles installed or licenses in use in the environment because of the complex dependencies and limitations involved in inventorying software license information for software titles installed in enterprise environments. Asset Intelligence reports should not be used as the sole source for determining purchased software license compliance.

Use the following procedure to view Asset Intelligence information by using the Asset Intelligence reports.

To view collected Asset Intelligence information by using Asset Intelligence reports

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, expand **Reporting**, expand **Reports**, and click **Asset Intelligence**. The Asset Intelligence reports are displayed.

   > **WARNING**
   >
   > If no report folders exist under the **Reports** node, verify that you have configured reporting. For more information, see Configuring reporting in System Center Configuration Manager.

3. Select the Asset Intelligence report that you want to run, and then on the **Home** tab, in the **Report Group** group, click **Run**.

Synchronize the Asset Intelligence catalog

You can synchronize the local Asset Intelligence catalog with System Center Online to retrieve the latest software title categorization. When you manually request catalog synchronization with System Center Online, it could take 15 minutes or longer to complete the synchronization process with System Center Online. Configuration Manager updates the **Last Successful Update** setting on the **Asset Intelligence** home page with the current time for when synchronization successfully finishes.

> **NOTE**
>
> An Asset Intelligence synchronization point site system role must first be installed before by using the procedures. For information about installing an Asset Intelligence synchronization point, see Configuring Asset Intelligence in System Center Configuration Manager.

Use the following procedure to create a synchronization schedule for the Asset Intelligence catalog.

To create a synchronization schedule for the Asset Intelligence catalog

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Asset Intelligence**.
3. On the **Home** tab, in the **Create** group, click **Synchronize**, and then click **Schedule Synchronization**.
4. In the **Asset Intelligence Synchronization Point Schedule** dialog box, select **Enable synchronization on a schedule**, and then configure a simple or custom schedule.
5. Click **OK** to save the changes.

> **NOTE**
>
> For information about the synchronization schedule, including the next scheduled synchronization, see the **Asset Intelligence** node in the **Assets and Compliance** workspace on the top-level site of the hierarchy.

Use the following procedure to manually synchronize the Asset Intelligence catalog.

> **WARNING**
>
> System Center Online accepts only one manual synchronization request in a 12-hour period.

To manually synchronize the Asset Intelligence catalog

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Asset Intelligence**.
3. On the **Home** tab, in the **Create** group, click **Synchronize**, click **Synchronize Asset Intelligence Catalog**, and then click **OK**.

Customize the Asset Intelligence catalog

Asset Intelligence catalog categorization information received from System Center Online is stored in the site database with read-only permissions and cannot be modified or deleted. However, you can create, modify, and delete custom software categories, software families, software labels, and hardware requirements catalog information. Then you can use custom categorization data instead of the information supplied by System Center Online for existing or user-defined software title information. When you change or add categorization information, the catalog information is considered user-defined. User-defined categorization information is stored in different database tables than validated catalog information.

Software categories

Asset Intelligence software categories are used to broadly categorize inventoried software titles and are also used as high-level groupings of more specific software families. For example, a software category could be energy companies, and a software family within that software category could be oil and gas or hydroelectric. Many software categories are predefined in the Asset Intelligence catalog, and additional user-defined categories can be created to further define inventoried software. The validation state for all predefined software categories is always **Validated**, while custom software category information added to the Asset Intelligence catalog is **User Defined**.

Use the following procedure to create a user-defined software category.

To create a user-defined software category

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Asset Intelligence**, and then click **Catalog**.
3. On the **Home** tab, in the **Create** group, click **Create Software Category**.
4. On the **General** page, enter a name for the new software category and, optionally, a description.

   > **NOTE**
   >
   > The validation state for all new custom software categories is always set to **User Defined**.

   Click **Next**.
5. On the **Summary** page, review the settings, and then click **Next**.

6. On the **Completion** page, click **Close** to exit the wizard.

Software families

Asset Intelligence software families are used to further define inventoried software titles within software categories. For example, a software category could be energy companies, and a software family within that software category could be oil and gas or hydroelectric. Many software families are predefined in the Asset Intelligence catalog, and additional user-defined families can be created to define inventoried software. The validation state for all predefined software families is always **Validated**, while custom software family information added to the Asset Intelligence catalog is **User Defined**.

Use the following procedure to create a user-defined software family.

To create a user-defined software family

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Asset Intelligence**, and then click **Catalog**.
3. On the **Home** tab, in the **Create** group, click **Create Software Family**.
4. On the **General** page, enter a name for the new software family and, optionally, a description.

   > **NOTE**
   > The validation state for all new custom software families is always set to **User Defined**.

5. On the **Summary** page, review the settings, and then click **Next**.
6. On the **Completion** page, click **Close** to exit the wizard.

Software labels

Asset Intelligence custom software labels let you create filters that you can use to group software titles and view them by using Asset Intelligence reports. For example, you can create a software label called shareware, associate it with a number of applications, and then run a report that shows you all titles with the software label of shareware. The validation state is **User Defined** for all custom software labels that you add to the Asset Intelligence catalog.

Use the following procedure to create a user-defined custom label.

To create a user-defined software label

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Asset Intelligence**, and then click **Catalog**.
3. On the **Home** tab, in the **Create** group, click **Create Software Label**.
4. On the **General** page, enter a name for the new software family and, optionally, a description.

   > **NOTE**
   > The validation state for all new custom software labels is always set to **User Defined**.

5. On the **Summary** page, review the settings, and then click **Next**.
6. On the **Completion** page, click **Close** to exit the wizard.

Hardware requirements

Hardware requirements information can help you verify that computers meet the hardware requirements for software titles before they are targeted for software deployments. Many hardware requirements are predefined in

the Asset Intelligence catalog, and you can create new user-defined hardware requirement information to meet custom requirements. The validation state for all predefined hardware requirements is always **Validated**, while user-defined hardware requirements information added to the Asset Intelligence catalog is **User Defined**.

> **IMPORTANT**
> The hardware requirements displayed in the Configuration Manager console are retrieved from the Asset Intelligence catalog on the local computer and are not based on inventoried software title information from System Center 2012 Configuration Manager clients. Hardware requirements information is not updated as part of the synchronization process with System Center Online. You can create user-defined hardware requirements for inventoried software that does not have associated hardware requirements.

Use the following procedure to create a user-defined hardware requirement.

To create a user-defined hardware requirements

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Asset Intelligence**, and then click **Hardware Requirements**.
3. On the **Home** tab, in the **Create** group, click **Create Hardware Requirements**.
4. On the **General** page, enter the following information:
   a. **Software title**: Specifies the software title for which the hardware requirements are associated. The software title cannot already exist in the Asset Intelligence catalog.
   b. **Validation state**: Lists the validation state as **User Defined** for the hardware requirements. You cannot modify this setting.
   c. **Minimum CPU (MHz)**: Specifies the minimum processor speed, in megahertz (MHz), required by the software title.
   d. **Minimum RAM (KB)**: Specifies the minimum RAM, in kilobytes (KB), required by the software title.
   e. **Minimum Disk Space (KB)**: Specifies the minimum free disk space, in KB, required by the software title.
   f. **Minimum Disk Size (KB)**: Specifies the minimum hard disk size, in KB, required by the software title.

   Click **Next**.
5. On the **Summary** page, review the settings, and then click **Next**.
6. On the **Completion** page, click **Close** to exit the wizard.

Modify categorization information for inventoried software

Predefined software in the Asset Intelligence catalog is configured with specific categorization information, such as product name, vendor, software category, and software family. When the predefined categorization information does not meet your requirements, you can modify the information in the properties for the software title. When you modify categorization information for predefined software, the validation state for the software changes from **Validated** to **User Defined**.

> **IMPORTANT**
> The categorization information can only be modified at the top-level site.

Use the following procedure to modify categorization information for inventoried software.

To modify the categorizations for software titles

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Asset Intelligence**, and then click **Inventoried Software**.
3. Select a software title or select multiple software titles for which you want to modify categorizations.
4. On the **Home** tab, in the **Properties** group, click **Properties**.
5. On the **General** tab, you can modify the following categorization information:
   - **Product Name**: Specifies the name of the inventoried software title.
   - **Vendor**: Specifies the name of the vendor that developed the inventoried software title.
   - **Category**: Specifies the software category that is currently assigned to the inventoried software title.
   - **Family**: Specifies the software family that is currently assigned to the inventoried software title.
6. Click **OK** to save the changes.

Use the following procedure to revert software to the original categorization information.

Revert categorization information to original settings for software

Configuration Manager stores categorization information obtained from System Center Online in the database. The information cannot be deleted. After the information has been modified, you can revert the categorization information back to the System Center Online categorization. Inventoried software that is not in the Asset Intelligence catalog can also be reverted back to the original settings.

Use the following procedure to revert categorization information to the original settings.

To revert categorization information to original settings

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Asset Intelligence**, and then click **Inventoried Software**.
3. Select a software title or select multiple software titles that you want to revert to the original settings. Only software that has a **User Defined** state can be reverted.

   > **TIP**
   > Click the **State** column to sort by the validation state. Sorting lets you see all software by validation state and quickly select multiple items to revert to the original settings.

4. On the **Home** tab, in the **Product** group, click **Revert**.
5. Click **Yes** to revert the software to the original categorization information.
6. When you revert categorization information for software that is in the Asset Intelligence catalog, the validation state changes from **User Defined** to **Validated**. When you revert software that is not in the catalog, the validation state changes from **User Defined** to **Uncategorized**.

Request a catalog update for uncategorized software titles

Uncategorized software title information can be submitted to System Center Online for research and categorization. After an uncategorized software title is submitted, and there are at least 4 categorization requests

from customers for the same software title, researchers identify, categorize, and then make the software title categorization information available to all customers that are using the System Center Online service. Microsoft gives the highest priority to software titles that have the most requests for categorization. Custom software and line-of-business applications are unlikely to receive a category, and as a best practice, you should not send these software titles to Microsoft for categorization.

When software title information is submitted to System Center Online for categorization, the following conditions apply:

- Only basic software title information is transmitted to System Center Online, and software title information to be categorized can be reviewed before submission.
- Software license information is never transmitted.
- Any software title that is uploaded becomes publicly available as part of the System Center Online catalog and can be downloaded by other customers.
- The source of the software title is not stored in the System Center Online catalog. However, application titles containing confidential or proprietary information should not be submitted for categorization by System Center Online.

> **NOTE**
> For more information about Asset Intelligence privacy information, see Security and privacy for Asset Intelligence in System Center Configuration Manager.

Use the following procedure to request Asset Intelligence catalog software title categorization from System Center Online.

To request a catalog update for uncategorized software titles

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Asset Intelligence**, and then click **Inventoried Software**.
3. Select a product name or select multiple product names, to be submitted to System Center Online for categorization. Only uncategorized inventoried software titles can be submitted to System Center Online for categorization. If an inventoried software title has been categorized by an administrator resulting in a user-defined state, you must right-click the inventoried software title, and then click **Revert** to revert the software title to the **Uncategorized** state before it can be submitted to System Center Online for categorization.

   > **NOTE**
   > Configuration Manager can process up to 2000 software titles for categorization at a time. If you select more than 2000 software titles, only the first 2000 software titles will be processed. You must select the remaining software titles for categorization in batches of less than 2000.

   > **TIP**
   > Click the **State** column to sort by the validation state. This lets you see all uncategorized product names and quickly select multiple items to submit for categorization.

4. On **Home** tab, in the **Product** group, click **Request Catalog Update**.
5. Review the System Center Online categorization submission privacy message. Click **Details** to view the

information that will be sent to System Center Online.

6. Select **I have read and understood this message**, and then click **OK** to allow the selected software titles to be submitted for categorization.

7. Verify that the state of the inventoried software product names submitted to System Center Online for categorization has changed from **Uncategorized** to **Pending**.

> **NOTE**
>
> Software that is submitted to System Center Online for categorization has a validation state of **Pending** on a central administration site is still displayed with a validation state of **Uncategorized** on child primary sites.

Resolve software details conflicts

After newly updated software categorization details have been received from System Center Online that conflict with existing software details information, you can choose how to resolve the conflict. Software that has a current conflict has a validation state of **Updatable**. After a software details conflict has been resolved, the software categorization information is retained in the Asset Intelligence catalog according to the setting that you specify. A software details conflict does not occur for the same software categorization value again unless the System Center Online value changes after the conflict has been resolved.

Use the following procedure to resolve a software details conflict.

To resolve a software details conflict

1. In the Configuration Manager console, click **Assets and Compliance**.

2. In the **Assets and Compliance** workspace, click **Asset Intelligence**, and then click **Inventoried Software**.

3. Review the **State** column for software titles in the **Updatable** state.

4. Select the software title for which you have to resolve a conflict, and then on the **Home** tab, in the **Product** group, and click **Resolve Conflict**.

5. Review the following information:

   - **Local value**: Specifies the existing software categorization information in the Asset Intelligence catalog that conflicts with newer System Center Online software categorization details.

   - **Downloaded value**: Specifies the new System Center Online software categorization information for conflicting Asset Intelligence catalog software categorization information.

6. Select one of the following settings to resolve the software details conflict:

   - **Do not change the locally edited catalog information value**: Resolves the software details conflict by retaining the existing Asset Intelligence catalog software categorization information. When you select this setting, the software title state changes from **Updatable** to **User Defined**.

   - **Overwrite the locally edited catalog information value with the downloaded System Center Online value**: Resolves the software details conflict by overwriting the existing Asset Intelligence catalog software categorization information with new information obtained from System Center Online. When you select this setting, the software title state changes from **Updatable** to **Validated**.

     Click **OK** to save the conflict resolution.

Security and privacy for Asset Intelligence in System Center Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This topic contains security and privacy information for Asset Intelligence in System Center Configuration Manager.

Security best practices for Asset Intelligence

Use the following security best practices for when you use Asset Intelligence.

SECURITY BEST PRACTICE	MORE INFORMATION
When you import a license file (Microsoft Volume Licensing file or a General License Statement file), secure the file and communication channel.	Use NTFS file system permissions to ensure that only authorized users can access the license files and use Server Message Block (SMB) signing to ensure the integrity of the data when it is transferred to the site server during the import process.
Use the principle of least permissions to import the license files.	Use role-based administration to grant the Manage Asset Intelligence permission to the administrative user who imports license files. The built-in role of Asset Manager includes this permission.

Privacy information for Asset Intelligence

Asset Intelligence extends the inventory capabilities of Configuration Manager to provide a higher level of asset visibility in the enterprise. Asset Intelligence information collection is not automatically enabled. You can modify the type of information collected by enabling hardware inventory reporting classes. For more information, see Configuring Asset Intelligence in System Center Configuration Manager.

Asset Intelligence information is stored in the Configuration Manager database in the same manner as inventory information. When clients connect to management points by using HTTPS, the data is always encrypted during transfer to the management point. When clients connect by using HTTP, you can configure the inventory data transfer to be signed and encrypted. Inventory data is not stored in encrypted format in the database. Information is retained in the database, until the site maintenance task **Delete Aged Inventory History** deletes it in intervals of every 90 days. You can configure the deletion interval.

Asset Intelligence does not send information about users and computers or license usage to Microsoft. You can choose to send System Center Online requests for categorization, which means that you can tag one or more software titles that are uncategorized and send them to System Center Online for research and categorization. After a software title is uploaded, Microsoft researchers identify, categorize, and then make that knowledge available to all customers who use the on-line service. You should be aware of the following privacy implications of submitting information to System Center Online:

- Upload applies only to generic software title information (name, publisher, and so on) that you choose to send to System Center Online. Inventory information is not sent with an upload.
- Upload never occurs automatically, and the system is not designed for this task to be automated. You must

manually select and approve the upload of each software title.

- A dialog box shows you exactly what data is going to be uploaded, before the upload process starts.
- License information is not sent to Microsoft. The license information is stored in a separate area of the Configuration Manager database, and it cannot be sent to Microsoft.
- Any software title that is uploaded becomes public, in the sense that the knowledge of that given application and its categorization become part of the System Center Online Asset Intelligence catalog, and then is downloaded to other consumers of the catalog.
- The source of the software title is not recorded in the Asset Intelligence catalog, and it is not made available to other customers. However, you must still verify that you do not load any application titles that contain any private information.
- Uploaded data cannot be recalled.

  Before you configure Asset Intelligence data collection and decide whether to submit information to System Center Online, consider the privacy requirements of your organization.

Example validation state transitions for Asset Intelligence

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Asset Intelligence validation states in Configuration Manager are not static and can change from administrative actions that you take to affect the data that are stored in the Asset Intelligence catalog. This topic provides examples for possible validation state transitions.

Uncategorized catalog item is categorized by the administrative user

STATE TRANSITION	STATE TRANSITION DESCRIPTION
Uncategorized	An inventoried software title that has not been previously categorized by System Center Online or that the administrative user has entered into the Asset Intelligence catalog.
Uncategorized to **UserDefined**	The uncategorized item is categorized by the administrative user.

Categorized catalog item is recategorized by the administrative user

STATE TRANSITION	STATE TRANSITION DESCRIPTION
Validated	Catalog item has been defined by System Center Online researchers and is present in the Asset Intelligence catalog.
Validated to **User Defined**	The validated catalog item is re-categorized by the administrative user.

> **NOTE**
> Because categorization information obtained from System Center Online is stored in the database and cannot be deleted, the administrative user can revert back to the System Center Online categorization later.

User-defined catalog item is recategorized by System Center Online

STATE TRANSITION	STATE TRANSITION DESCRIPTION
Uncategorized	An inventoried software title is entered into the Asset Intelligence catalog that has not been previously categorized by System Center Online or the administrative user.
User Defined	The uncategorized item is categorized by the administrative user.

STATE TRANSITION	STATE TRANSITION DESCRIPTION
User Defined to **Updateable**	A user-defined catalog item has been categorized differently by System Center Online during subsequent manual bulk updates of the Asset Intelligence catalog. The administrative user can use the **Software Details Conflict Resolution** dialog box to decide whether to use the new categorization information or the previous user-defined value.
Updateable to **Validated**	The administrative user uses the **Software Details Conflict Resolution** dialog box to use the new categorization information received from System Center Online during the previous catalog update.
or	
Updateable to **User Defined**	The administrative user uses the **Software Details Conflict Resolution** dialog box to use the previous user-defined value.

NOTE

Because categorization information obtained from System Center Online is stored in the database and cannot be deleted, the administrative user can revert back to the System Center Online categorization later.

Uncategorized catalog item is submitted to System Center Online for categorization

STATE TRANSITION	STATE TRANSITION DESCRIPTION
Uncategorized	An inventoried software title is entered into the Asset Intelligence database that has not been previously categorized by System Center Online or the administrative user.
Uncategorized to **Pending**	The uncategorized item is submitted to System Center Online for categorization by the administrative user.
Pending to **Validated**	The item is categorized by System Center Online. The administrative user imports the item into the Asset Intelligence catalog by using a bulk catalog update or Asset Intelligence catalog synchronization. Both are available by using the Asset Intelligence synchronization point site system role.

User-defined catalog item is submitted to System Center Online for categorization

STATE TRANSITION	STATE TRANSITION DESCRIPTION
Uncategorized	An inventoried software title is entered into the Asset Intelligence database that has not been previously categorized by an administrative user or System Center Online.

STATE TRANSITION	STATE TRANSITION DESCRIPTION
User Defined	You categorized the uncategorized item.
User Defined to **Pending**	You submit the user-defined item to System Center Online for categorization.
Pending to **Updateable**	A user-defined catalog item has been categorized differently by System Center Online during subsequent catalog synchronization. You can use the **Resolve Conflict** action to decide whether to use the new categorization information or the previous user-defined value. For more information about resolving conflicts, see Resolve software details conflicts.
Updateable to **Validated**	You use the **Resolve Conflict** action and select the new categorization information received from System Center Online during the previous catalog update. For more information about resolving conflicts, see Resolve software details conflicts.
or	
Updateable to **User Defined**	You use the **Resolve Conflict** action and select to use the previous user-defined value. For more information about resolving conflicts, see Resolve software details conflicts.

NOTE

Because categorization information obtained from System Center Online is stored in the database and cannot be deleted, you can revert back to the System Center Online categorization later.

Example Asset Intelligence general license import file in System Center Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

The example information in this topic can be used to create a sample general software license file to import software licenses into the Asset Intelligence catalog by using the Import Software License Wizard. You can copy and paste the following table into a new Microsoft Excel spreadsheet and save it with a .csv file name extension to be used as an example general software license import file for testing purposes. When creating the license import file, all header fields are required while only Name, Publisher, Version, and EffectiveQuantity data values are required in the spreadsheet. For more information about importing software licenses to the Asset Intelligence catalog, see Configuring Asset Intelligence in System Center Configuration Manager.

NAME	PUBLISHER	VERSION	LANGUAGE	EFFECTIVEQUANTITY	PONUMBER	RESELLERNAME	DATEOFPURCHASE	SUPPORTPURCHASED	SUPPORTEXPIRATIONDATE	COMMENTS
Software Title 1	Software publisher	1.01	English	1	Purchase number	Reseller name	10/10/2010	0	10/10/2012	Comment
Software title 2	Software publisher	1.02	English	1	Purchase number	Reseller name	10/10/2010	0	10/10/2012	Comment
Software title 3	Software publisher	1.03	English	1	Purchase number	Reseller name	10/10/2010	0	10/10/2012	Comment
Software title 4	Software publisher	1.04	English	1	Purchase number	Reseller name	10/10/2010	0	10/10/2012	Comment
Software title 5	Software publisher	1.05	English	1	Purchase number	Reseller name	10/10/2010	0	10/10/2012	Comment
Software title 6	Software publisher	1.06	English	1	Purchase number	Reseller name	10/10/2010	0	10/10/2012	Comment
Software title 7	Software publisher	1.07	English	1	Purchase number	Reseller name	10/10/2010	0	10/10/2012	Comment

NAME	PUBLISHER	VERSION	LANGUAGE	EFFECTIVEQUANTITY	PONUMBER	RESELLERNAME	DATEOFPURCHASE	SUPPORTPURCHASED	SUPPORTEXPIRATIONDATE	COMMENTS
Software title 8	Software publisher	1.08	English	1	Purchase number	Reseller name	10/10/2010	0	10/10/2012	Comment
Software title 9	Software publisher	1.09	English	1	Purchase number	Reseller name	10/10/2010	0	10/10/2012	Comment
Software title 10	Software publisher	1.10	English	1	Purchase number	Reseller name	10/10/2010	0	10/10/2012	Comment

Manage Microsoft Lifecycle Policy with Configuration Manager

5/15/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Beginning with version 1806, you can use the Configuration Manager product lifecycle dashboard to view the Microsoft Lifecycle Policy. The dashboard shows the state of the Microsoft Lifecycle Policy for Microsoft products installed on devices managed with Configuration Manager. It also provides you with information about Microsoft products in your environment, supportability state, and support end dates. Use the dashboard to understand the availability of support for each product. This information helps you plan for when to update the Microsoft products you use before their current end of support is reached.

For more information, see the Microsoft Lifecycle Policy.

Starting in version 1810, the dashboard includes information for System Center 2012 Configuration Manager and later.

Prerequisites

To see data in the product lifecycle dashboard, the following components are required:

- Internet Explorer 9 or later must be installed on the computer running the Configuration Manager console.
- A service connection point role must be installed and configured. To get updates for the data on this dashboard, the service connection point must be online, or synchronized regularly if offline. For more information, see About the service connection point.
- A reporting services point is required for hyperlink functionality in the dashboard. The dashboard links to SQL Server Reporting Services (SSRS) reports. For more information, see Reporting in Configuration Manager.
- The asset intelligence synchronization point must be configured and synchronized. The dashboard uses the asset intelligence catalog as metadata for product titles. The metadata is compared against inventory data in your hierarchy. For more information, see Configure asset intelligence in Configuration Manager.

> **NOTE**
> If you're configuring the asset intelligence service point for the first time, make sure to enable asset intelligence hardware inventory classes. The lifecycle dashboard depends on those asset intelligence hardware inventory classes. The dashboard won't display data until clients have scanned for and returned hardware inventory.

Use the product lifecycle dashboard

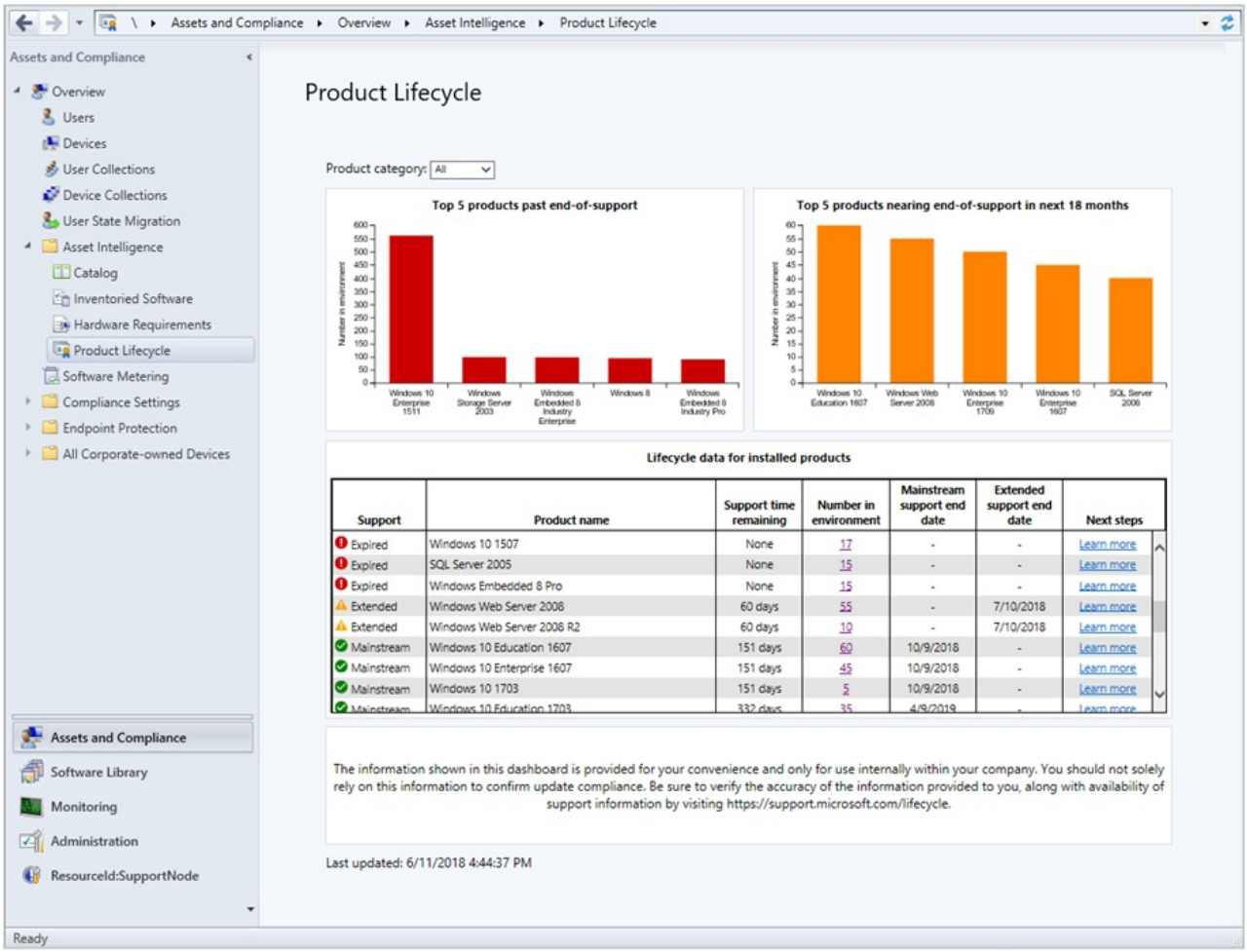
Based on inventory data the site collects from managed devices, the dashboard displays information about all current products. However, the information displayed for operating systems and SQL Server is limited to the following versions:

- Windows Server 2008 and later
- Windows XP and later
- SQL Server 2008 and later

To access the lifecycle dashboard in the Configuration Manager console, go to the **Assets and Compliance** workspace, expand **Asset Intelligence**, and select the **Product Lifecycle** node.

> **NOTE**
>
> The data in the dashboard is based on the site the Configuration Manager console connects to. If the console connects to your top-tier site, you see data for the entire hierarchy. When connected to a child primary site, only data from that site displays.

Product lifecycle dashboard



Change the view by selecting one of the following options from the **Product category** list:

- **All**: View all products together
- **Windows Client**: View Windows client OS versions
- **Windows Server**: View Windows server OS versions
- **Database**: View SQL Server versions
- **Configuration Manager**: Starting in version 1810, view Configuration Manager versions
- **Microsoft Office**: Starting in version 1902, view information for installed versions of Office 2003 through Office 2016

The dashboard has the following tiles:

- **Top five products past end-of-life**: This tile is a consolidated data view of products found in your environment past their end-of-life. The graph shows installed software that's expired when compared against the support lifecycle for operating systems and SQL server products.
- **Top five products nearing end-of-life**: This tile is a consolidated data view of products found in your environment that are nearing end-of-life in next eighteen months. The graph shows installed software that's

within eighteen months of end-of-life when compared against the support lifecycle for operating systems and SQL server products.

- **Lifecycle data for installed products**: This tile gives you a general idea of when a product transitions from supported to the expired state. The chart provides a breakdown of the number of clients where the product is installed, the support availability state, and a link to learn more about the next steps to take. The following information is included in the chart:
  - Support time remaining
  - Number in environment
  - Mainstream support end date
  - Extended support end date
  - Next steps

> **IMPORTANT**
> The information shown in this dashboard is provided for your convenience and only for use internally within your company. You should not solely rely on this information to confirm compliance. Be sure to verify the accuracy of the information provided to you, along with availability of support information by visiting the Microsoft Lifecycle Policy.

Reporting

Additional reports are available as well. In the Configuration Manager console, go to the **Monitoring** workspace, expand **Reporting**, and expand **Reports**. The following new reports are added under the category **Asset Intelligence**:

- **Lifecycle 01A - Computers with a specific software product**: View a list of computers on which a specified product is detected.
- **Lifecycle 02A - List of machines with expired products in the organization**: View computers that have expired products on them. You can filter this report by product name.
- **Lifecycle 03A - List of expired products found in the organization**: View details for products in your environment that have expired lifecycle dates.
- **Lifecycle 04A - General Product Lifecycle overview**: View a list of product lifecycles. Filter the list by product name and days to expiration.
- **Lifecycle 05A - Product lifecycle dashboard**: Starting in version 1810, this report includes similar information as the in-console dashboard. Select a category to view the count of products in your environment, and the days of support remaining.

For more information, see List of reports.

Introduction to remote control in System Center Configuration Manager

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use remote control to remotely administer, provide assistance, or view any client computer in the hierarchy. You can use remote control to troubleshoot hardware and software configuration problems on client computers and to provide support. Configuration Manager supports the remote control of all workgroup computers and domain-joined computers that run supported operating systems for the Configuration Manager client. For more information, see Supported operating systems for clients and devices for System Center Configuration Manager

Configuration Manager also lets you configure client settings to run Windows Remote Desktop and Remote Assistance from the Configuration Manager console.

> **NOTE**
> You cannot establish a Remote Assistance session from the Configuration Manager console to a client computer that is in a workgroup.

You can start a remote control session in the Configuration Manager console from **Assets and Compliance** > **Devices**, from any device collection, from the Windows Command Prompt window, or from the Windows **Start** menu.

Prerequisites for remote control in System Center Configuration Manager

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Remote control in System Center Configuration Manager has external dependencies and dependencies in the product.

Dependencies external to Configuration Manager

DEPENDENCY	MORE INFORMATION
Computer video card driver	Ensure that the most up-to-date video driver is installed on client computers to ensure optimal remote control performance.

Devices that run Windows Embedded, Windows Embedded for Point of Service (POS), and Windows Fundamentals for Legacy PCs do not support the remote control viewer, but they do support the remote control client.

Configuration Manager remote control cannot be used to remotely administer client computers that run Systems Management Server 2003 or Configuration Manager 2007.

> **NOTE**
> No Windows services are required as an external dependency for remote control.

Supported operating systems for the remote control viewer

The remote control viewer is supported on all operating systems that are supported for the Configuration Manager console. For information, see Supported configurations for System Center Configuration Manager consoles.

Configuration Manager dependencies

DEPENDENCY	MORE INFORMATION
Remote control must be enabled for clients	By default, remote control is not enabled when you install Configuration Manager. For information about how to enable and configure remote control, see Configuring remote control in System Center Configuration Manager.
Reporting services point	The reporting services point site system role must be installed before you can run reports for remote control. For more information, see Reporting in System Center Configuration Manager.

DEPENDENCY	MORE INFORMATION
Security permissions to manage remote control	To access collection resources and to initiate a remote control session from the Configuration Manager console: **Read**, **Read Resource**, and **Remote Control** permission for the **Collection** object. The **Remote Tools Operator** security role includes these permissions that are required to manage remote control in Configuration Manager. For more information, see Configure role-based administration for System Center Configuration Manager. Additionally, permitted viewers must be given permission to use remote control by adding these users to the **Permitted viewers of Remote Control and Remote Assistance** list in the **Remote Tools** client settings.

Configuring remote control in System Center Configuration Manager

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This procedure describes configuring the default client settings for remote control. These settings apply to all computers in your hierarchy. If you want these settings to apply to only some computers, assign a custom device client setting to a collection that contains those computers. For more information a see How to configure client settings in System Center Configuration Manager.

To use Remote Assistance or Remote Desktop, it must be installed and configured on the computer that runs the Configuration Manager console. For more information about how to install and configure Remote Assistance or Remote Desktop, see your Windows documentation.

To enable remote control and configure client settings

1. In the Configuration Manager console, choose **Administration** > **Client Settings** > **Default Client Settings**.
2. On the **Home** tab, in the **Properties** group, choose **Properties**.
3. In the **Default** dialog box, choose **Remote Tools**.
4. Configure the remote control, Remote Assistance and Remote Desktop client settings. For a list of remote tools client settings that you can configure, see Remote Tools.

   You can change the company name that appears in the **ConfigMgr Remote Control** dialog box by configuring a value for **Organization name displayed in Software Center** in the **Computer Agent** client settings.

   Client computers are configured with these settings the next time they download client policy. To initiate policy retrieval for a single client, see How to manage clients in System Center Configuration Manager.

Enable keyboard translation

By default, Configuration Manager transmits the key position from the viewer's location to the sharer's location. This can present a problem for keyboard configurations that differ from viewer to sharer. For example, a viewer with an English keyboard would type an "A", but the sharer's French keyboard would provide a "Q". You now have the option of configuring remote control so that the character itself is transmitted from the viewer's keyboard to the sharer, and what the viewer intends to type arrives at the sharer.

To turn on keyboard translation, in **Configuration Manager Remote Control**, choose **Action**,and choose **Enable keyboard translation** to transmit key position.

> **NOTE**
> Special keys, such as ~!#@$%, will not be translated correctly.

Keyboard shortcuts for the remote control viewer

KEYBOARD SHORTCUT	DESCRIPTION
Alt+Page Up	Switches between running programs from left to right.
Alt+Page Down	Switches between running programs from right to left.
Alt+Insert	Cycles through running programs in the order that they were opened.
Alt+Home	Displays the **Start** menu.
Ctrl+Alt+End	Displays the Windows Security dialog box (Ctrl+Alt+Del).
Alt+Delete	Displays the Windows menu.
Ctrl+Alt+Minus Sign (on the numeric keypad)	Copies the active window of the local computer to the remote computer Clipboard.
Ctrl+Alt+Plus Sign (on the numeric keypad)	Copies the entire local computer's window area to the remote computer Clipboard.

How to remotely administer a Windows client computer by using System Center Configuration Manager

7/9/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch) Configuration Manager allows you to connect to client computers using **Configuration Manager Remote Control**. Before you begin to use remote control, ensure that you review the information in the following articles:

- Prerequisites for remote control in System Center Configuration Manager
- Configuring remote control in System Center Configuration Manager

Here are three ways to start the remote control viewer:

- In the Configuration Manager console.
- In a Windows command prompt.
- From the Windows **Start** menu, on a computer that runs the Configuration Manager console, in the **Microsoft System Center** program group.

To remotely administer a client computer from the Configuration Manager console

1. In the Configuration Manager console, choose **Assets and Compliance** > **Devices** or **Device Collections**.
2. Select the computer that you want to remotely administer and then, in the **Home** tab, in the **Device** group, choose **Start** > **Remote Control**.

   > **IMPORTANT**
   > If the client setting **Prompt user for Remote Control** permission is set to **True**, the connection does not initiate until the user at the remote computer agrees to the remote control prompt. For more information, see Configuring remote control in System Center Configuration Manager.

3. After the **Configuration Manager Remote Control** window opens, you can remotely administer the client computer. Use the following options to configure the connection.

   > **NOTE**
   > If the computer that you connect to has multiple monitors, the display from all the monitors is shown in the remote control window.

   - **File**
     - **Connect** - Connect to another computer. This option is unavailable when a remote control session is active.
     - **Disconnect** - Disconnects the active remote control session but doesn't close the **Configuration Manager Remote Control** window.

- **Exit** - Disconnects the active remote control session and closes the **Configuration Manager Remote Control** window.

> **NOTE**
> When you disconnect a remote control session, the contents of the Windows Clipboard on the computer that you are viewing is deleted.

- **View**
  - **Color depth** - Choose either 16 bits or 32 bits per pixel.
  - **Full Screen** - Maximizes the **Configuration Manager Remote Control** window. To exit full screen mode, press Ctrl+Alt+Break.
  - **Optimize for low bandwidth connection** - Choose this option if the connection is low bandwidth.
  - **Display:**
    - **All Screens** - Added in Configuration Manager 1902. If the computer that you connect to has multiple monitors, the display from all the monitors is shown in the remote control window. **All Screens** is the only view for computers with multiple monitors before 1902.
    - **First Screen** - Added in Configuration Manager 1902. The *first screen* is at the top and far left as shown in Windows display settings. You can't select a specific screen. When you switch the configuration of the viewer, reconnect the remote session. The viewer saves your preference for future connections.
    - **Scale to Fit** - Scales the display of the remote computer to fit the size of the **Configuration Manager Remote Control** window.
    - **Status Bar** - Toggles the display of the **Configuration Manager Remote Control** window status bar.

> **NOTE**
> The viewer saves your preference for future connections.

- **Action**
  - **Send Ctrl+Alt+Del Key** - Sends a Ctrl+Alt+Del key combination to the remote computer.
  - **Enable Clipboard Sharing** - Lets you copy and paste items to and from the remote computer. If you change this value, you must restart the remote control session for the change to take effect.
    - If you don't want clipboard sharing to be enabled in the Configuration Manager console, on the computer running the console, set the value of the registry key **HKEY_CURRENT_USER\Software\Microsoft\ConfigMgr10\Remote Control\Clipboard Sharing** to **0**.
  - **Enable Keyboard Translation** - Translates the keyboard layout of the computer running the console to the connected device's layout.
  - **Lock Remote Keyboard and Mouse** - Locks the remote keyboard and mouse to prevent the user from operating the remote computer.
- **Help**
  - **About Remote Control** - Displays the current version of the viewer.

4. Users at the remote computer can view more information about the remote control session when they click the Configuration Manager**Remote Control** icon. The icon is in the Windows notification area or the icon on the remote control session bar.

To start the remote control viewer from the Windows command line

- At the Windows command prompt, type <*Configuration Manager Installation Folder*>**\AdminConsole\Bin\x64\CmRcViewer.exe**

CmRcViewer.exe supports the following command-line options:

- *Address* - Specifies the NetBIOS name, the fully qualified domain name (FQDN), or the IP address of the client computer that you want to connect to.
- *Site Server Name* - Specifies the name of the System Center Configuration Manager site server to which you want to send status messages that are related to the remote control session.
- **/?** - Displays the command-line options for the remote control viewer.

Example:CmRcViewer.exe <*Address*> <*Site Server Name*>

How to audit remote control usage in System Center Configuration Manager

5/9/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can use System Center Configuration Manager reports to view audit information for remote control.

For more information about how to configure reporting in Configuration Manager, see Reporting in System Center Configuration Manager.

The following two reports are available with the category **Status Messages - Audit**:

- **Remote Control - All computers remote controlled by a specific user** - Displays a summary of remote control activity that a specific user initiated.
- **Remote Control - All remote control information** - Displays a summary of status messages about remote control of client computers.

To run the report Remote Control - All computers remote controlled by a specific user

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, expand **Reporting**, and then click **Reports**.
3. In the **Reports** node, click the **Category** column to sort the reports so that you can more easily find the reports in the category **Status Messages - Audit**.
4. Select the report **Remote Control - All computers remote controlled by a specific user**, and then, on the **Home** tab, in the **Report Group**, click **Run**.
5. In the **User Name** list of the **Remote Control - All computers remote controlled by a specific user**, specify the user that you want to report audit information for, and then click **View Report**.
6. When you have finished viewing the data in the report, close the report window.

To run the report Remote Control - All remote control information

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, expand **Reporting**, and then click **Reports**.
3. In the **Reports** node, click the **Category** column to sort the reports so that you can more easily find the reports in the category **Status Messages - Audit**.
4. Select the report **Remote Control - All remote control information**, and then, on the **Home** tab, in the **Report Group**, click **Run** to open the **Remote Control - All remote control information** window.
5. When you have finished viewing data in the report, close the report window.

Security and privacy for remote control in System Center Configuration Manager

5/9/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This topic contains security and privacy information for remote control in System Center Configuration Manager.

Security best practices for remote control

Use the following security best practices when you manage client computers by using remote control.

SECURITY BEST PRACTICE	MORE INFORMATION
When you connect to a remote computer, do not continue if NTLM instead of Kerberos authentication is used.	When Configuration Manager detects that the remote control session is authenticated by using NTLM instead of Kerberos, you see a prompt that warns you that the identity of the remote computer cannot be verified. Do not continue with the remote control session. NTLM authentication is a weaker authentication protocol than Kerberos and is vulnerable to replay and impersonation.
Do not enable Clipboard sharing in the remote control viewer.	The Clipboard supports objects such as executable files and text and could be used by the user on the host computer during the remote control session to run a program on the originating computer.
Do not enter passwords for privileged accounts when remotely administering a computer.	Software that observes keyboard input could capture the password. Or, if the program that is being run on the client computer is not the program that the remote control user assumes, the program might be capturing the password. When accounts and passwords are required, the end user should enter them.
Lock the keyboard and mouse during a remote control session.	If Configuration Manager detects that the remote control connection is terminated, Configuration Manager automatically locks the keyboard and mouse so that a user cannot take control of the open remote control session. However, this detection might not occur immediately and does not occur if the remote control service is terminated. Select the action **Lock Remote Keyboard and Mouse** in the **ConfigMgr Remote Control** window.
Do not let users configure remote control settings in Software Center.	Do not enable the client setting **Users can change policy or notification settings in Software Center** to help prevent users from being spied on. If one user changes it, it can allow a different user on the same machine to be viewed remotely. **This setting is for the computer, not for the logged-on user**.

SECURITY BEST PRACTICE	MORE INFORMATION
Enable the **Domain** Windows Firewall profile.	Enable the client setting **Enable remote control on clients Firewall exception profiles** and then select the **Domain** Windows Firewall for intranet computers.
If you log off during a remote control session and log on as a different user, ensure that you log off before you disconnect the remote control session.	If you do not log off in this scenario, the session remains open.
Do not give users local administrator rights.	When you give users local administrator rights, they might be able to take over your remote control session or compromise your credentials.
Use either Group Policy or Configuration Manager to configure Remote Assistance settings, but not both.	You can use Configuration Manager and Group Policy to make configuration changes to the Remote Assistance settings. When Group Policy is refreshed on the client, by default, it optimizes the process by changing only the policies that have changed on the server. Configuration Manager changes the settings in the local security policy, which might not be overwritten unless the Group Policy update is forced. Setting policy in both places might lead to inconsistent results. Choose one of these methods to configure your Remote Assistance settings.
Enable the client setting **Prompt user for Remote Control permission**.	Although there are ways around this client setting that prompts a user to confirm a remote control session, enable this setting to reduce the chance of users being spied upon while working on confidential tasks. In addition, educate users to verify the account name that is displayed during the remote control session and disconnect the session if they suspect that the account is unauthorized.
Limit the Permitted Viewers list.	Local administrator rights are not required for a user to be able to use remote control.

Security issues for remote control

Managing client computers by using remote control has the following security issues:

- Do not consider remote control audit messages to be reliable.

  If you start a remote control session and then log on by using alternative credentials, the original account sends the audit messages, not the account that used the alternative credentials.

  Audit messages are not sent if you copy the binary files for remote control rather than install the Configuration Manager console, and then run remote control at the command prompt.

Privacy information for remote control

Remote control lets you view active sessions on Configuration Manager client computers and potentially view any information stored on those computers. By default, remote control is not enabled.

Although you can configure remote control to provide prominent notice and get consent from a user before a remote control session begins, it can also monitor users without their permission or awareness. You can configure View Only access level so that nothing can be changed on the remote control, or Full Control. The account of the connecting administrator is displayed in the remote control session, to help users identify who is connecting to

their computer.

By default, Configuration Manager grants the local Administrators group Remote Control permissions.

Before you configure remote control, consider your privacy requirements.

Introduction to power management in System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Power Management in System Center Configuration Manager addresses the need that many organizations have to monitor and reduce the power consumption of their computers. The feature takes advantage of the power management features built into Windows to apply relevant and consistent settings to computers in the organization. You can apply different power settings to computers during business hours and nonbusiness hours. For example, you might want to apply a more restrictive power plan to computers during nonbusiness hours. In cases where computers must always remain turned on, you can prevent power management settings from being applied.

Power management in Configuration Manager includes several reports to help you analyze power consumption and computer power settings in your organization. You can also use the reports to help you troubleshoot problems with power management.

For a detailed workflow about how to configure and use power management, see Administrator checklist for power management in System Center Configuration Manager.

> **IMPORTANT**
> Configuration Manager power management is not supported on virtual machines. You cannot apply power plans to virtual machines, nor can you or report power data from them.

The power management workflow

Use the following three phases to plan and implement power management in Configuration Manager.

Monitoring and planning phase

Power Management uses Configuration Manager hardware inventory to collect data about computer usage and power settings for computers in the site. There are a number of reports that you can use to analyze this data and determine the optimal power management settings for computers. For example, during the monitoring and planning phase of the power management workflow, you can create collections that are based on the data that is included in the **Power Capabilities** report and use that data to identify the computers that are not capable of power management. Then, you can exclude those computers from power management.

> **IMPORTANT**
> Do not apply power plans to computers in your site until you collect and analyze the power data from client computers. If you apply new power management settings to computers without first examining the existing settings, you might experience an increase in power consumption.

Enforcement phase

Power management lets you create power plans that you can apply to collections of computers in your site. These power plans configure Windows power management settings on computers. You can use the power plans that are included with Configuration Manager, or you can configure your own custom power plans. You can use the power data that is collected during the monitoring and planning phase as a baseline to help you evaluate power savings

after you apply a power plan to computers. For more information, see Administrator checklist for power management in System Center Configuration Manager.

Compliance phase

In the compliance phase, you can run reports that help you to evaluate power usage and power cost savings in your organization. You can also run reports that describe the improvements in the amount of CO2 generated by computers. Reports are also available that help you validate that power settings were correctly applied to computers and that help you troubleshoot problems with the power management feature.

Prerequisites for power management in System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Power management in System Center Configuration Manager has external dependencies and dependencies within the product.

Dependencies external to Configuration Manager

The following table lists the dependencies external to Configuration Manager for using power management.

DEPENDENCY	MORE INFORMATION
Client computers must be able to support the required power states	To use all features of power management, client computers must be able to support the sleep, hibernate, wake from sleep, and wake from hibernate actions. You can use the **Power Capabilities** report to determine if computers can support these actions. For more information, see Power Capabilities report in the topic How to monitor and plan for power management in System Center Configuration Manager.

Configuration Manager dependencies

The following table lists the dependencies within Configuration Manager for using power management.

DEPENDENCY	MORE INFORMATION
Power management must be enabled before you can create and monitor power plans.	For information about how to enable and configure power management, see Configuring power management in System Center Configuration Manager.
Reporting services point	You must configure a reporting services point before you can view power management reports. For more information, see Reporting in System Center Configuration Manager.

Recommendations for power management in Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the following recommendations for power management in Configuration Manager.

Monitor at a representative time

The monitoring phase of power management provides you with the following information from computers in your organization:

- Power consumption
- Activity
- Power management capabilities
- Environmental impact

Choose a representative time to monitor the devices. For example, monitoring during a public holiday doesn't provide a realistic report on computer power usage.

Create a control collection

Create two collections of computers to help you monitor the effects of applying power plans to computers. The first collection should contain the majority of the computers to which you want to apply power settings. The *control collection* should contain the remaining computers. Apply the required power management plan to the first collection. Then run reports to compare the impact between the two collections.

Run reports before you apply a plan

Before you apply a power management plan to a collection of computers, run the **Power Settings** report. Use this report to help you understand the power management settings that are already configured on computers in the collection. If you apply new power management settings to computers without first examining the existing settings, it might increase their power consumption.

Exclude servers

Power management for computers that run Windows Server isn't supported. Add servers to a collection and exclude it from power management.

> **NOTE**
> Although Configuration Manager doesn't support power management of Windows Server, it still collects power usage data for analysis and reporting.

Exclude other computers

If you have computers that you don't want to manage with power management, add these computers to an exclusion collection.

You might want to exclude from power management the following types of computers:

- Computers that must remain turned on.
- Computers that users need to connect to remotely.
- Computers that can't use power management.
- Computers that have the distribution point site system role.
- Public computers such as kiosk computers, information displays, or monitoring consoles where the computer and the monitor must always be turned on.

For more information, see Configuring power management.

Apply power plans to a test collection

Always test the effect of applying a power management plan on a test collection of computers before you apply the power plan to a larger collection of computers.

When you exclude a computer from power management, all power settings revert to their original values. You can't revert individual power settings to their original values.

Apply power plan settings individually

Monitor the effect of applying each power setting before you apply the next one. This process makes sure that each setting has the required effect. For more information about power plan settings, see Available power management plan settings.

Regularly monitor computers for multiple power plans

Power management includes a report that displays computers that have more than one power plan applied: **Computers with Multiple Power Plans**.

If a computer is a member of multiple collections, each applying different power plans, then the following behaviors apply:

- **Power plan**: If you apply multiple values for power settings to a computer, it uses the least restrictive value.
- **Wakeup time**: If you apply multiple wakeup times to a desktop computer, it uses the time closest to midnight.

For more information, see Computers with multiple power plans.

Save or export power management information

When you run reports during the monitoring and compliance phases, save or export the results. Keep the data for later comparison in case Configuration Manager later removes the data.

Configuration Manager keeps in the site database the following power management information:

- Power management information used by daily reports: 31 days
- Power management information used by monthly reports: 13 months

Administrator checklist for power management in System Center Configuration Manager

2/12/2019 • 5 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This administrator checklist provides the recommended steps for using System Center Configuration Manager power management in your organization.

Configuring power management

Use these steps to help you configure your hierarchy to collect power management information from client computers.

> **IMPORTANT**
> Do not apply power plans to computers in your hierarchy until you have collected and analyzed power data from client computers. If you apply new power management settings to computers without first examining the existing settings, this might lead to an increase in power consumption.

TASK	DETAILS
Review the power management concepts in the Configuration Manager documentation library.	See Introduction to power management.
Review the power management prerequisites in the Configuration Manager documentation library.	See Prerequisites for power management.
Review the best practices information for power management.	See Best practices for power management.
Configure your collections to manage power consumption from computers within your environment.	Use the **Collection for reporting of baseline data**, **Collection for reporting of baseline data**, **Collection of computers incapable of power management**, **Collections of computers to which power plans will be applied**, **Collections of computers to which power plans will be applied**, and **Collections of computers that are running Windows Server** to help you manage power settings for computers in your hierarchy. You can create multiple collections and apply different power plans to each collection.
Enable power management.	Before you can begin to use power management, you must enable it and configure the required client settings. For more information, see Configuring power management.
Collect power management information from client computers.	Power management data is reported by clients through Configuration Manager hardware inventory. Depending on the hardware inventory schedule that you have configured, it might take some time to retrieve inventory from all client computers.

Monitoring and planning phase

TASK	DETAILS
Run the report **Computer Activity**.	The **Computer Activity** report displays a graph showing monitor, computer, and user activity for a specified collection over a specified time period. This report links to the **Computer Activity Details** report which displays the sleep and wake capabilities of computers in the specified collection. For more information, see How to monitor and plan for power management.
Run the report **Energy Consumption** or **Energy Consumption by Day**.	The **Energy Consumption** and **Energy Consumption by Day** reports display the total monthly power consumption in kilowatt per hour (kWh) for a specified collection over a specified time period. For more information, see How to monitor and plan for power management.
Run the report **Environmental Impact** or **Environmental Impact by Day**.	The **Environmental Impact** and **Environmental Impact by Day** reports display a graph showing carbon dioxide (CO2) emissions saved by a specified collection of computers for a specified period of time. For more information, see How to monitor and plan for power management.
Run the report **Energy Cost** or **Energy Cost by Day**.	The **Energy Cost** and **Energy Cost by Day** reports display the total power consumption cost for a specified period of time. For more information, see How to monitor and plan for power management.
Run the report **Power Capabilities**.	The **Power Capabilities** report displays the power management capabilities of computers in the specified collection. For more information, see How to monitor and plan for power management.
Run the report **Power Settings**.	The **Power Settings** report displays an aggregated list of the current power settings used by computers in a specified collection. For more information, see How to monitor and plan for power management.
Exclude any required collections of computers from power management.	See Configuring power management.

IMPORTANT

Ensure that you save the information from power management reports generated during the monitoring and planning phase. You can compare this data to power management information generated during the enforcement and compliance phases to help you evaluate, the power usage, power cost and environmental impact savings from applying a power plan to computers in your hierarchy.

Enforcement phase

TASK	DETAILS
Select existing power plans or create new power plans for collections of computers in your organization.	See How to create and apply power plans.

TASK	DETAILS
Apply these power plans to computers.	See How to create and apply power plans.

Compliance phase

TASK	DETAILS
Run the report **Computer Activity**.	The **Computer Activity** report displays a graph showing monitor, computer, and user activity for a specified collection over a specified time period. This report links to the **Power Computer Activity Details** report which displays the sleep and wake capabilities of computers in the specified collection. For more information, see How to monitor and plan for power management.
Run the report **Energy Consumption** or **Energy Consumption by Day**.	The **Energy Consumption** and **Energy Consumption by Day** reports display the total monthly power consumption in kilowatt per hour (kWh) for a specified collection over a specified time period. For more information, see How to monitor and plan for power management.
Run the report **Environmental Impact** or **Environmental Impact by Day**.	The **Environmental Impact** and **Environmental Impact by Day** reports display a graph showing carbon dioxide (CO2) emissions saved by a specified collection of computers for a specified period of time. For more information, see How to monitor and plan for power management.
Run the report **Energy Cost** or **Energy Cost by Day**.	The **Energy Cost** and **Energy Cost by Day** reports display the total power consumption cost for a specified period of time. For more information, see How to monitor and plan for power management.

Troubleshooting

TASK	DETAILS
If computers in your hierarchy have not entered sleep or hibernate, run the report **Insomnia Report** to display possible causes.	The **Insomnia Report** displays a list of common causes that prevented computers from entering sleep or hibernate and the number of computers affected by each cause for a specified time period. For more information, see How to monitor and plan for power management.
If multiple power plans are applied to one computer, then the least restrictive power plan is applied. Run the report **Computers with Multiple Power Plans** to see computers with multiple power plans applied.	See **Computers with Multiple Power Plans** in How to monitor and plan for power management.

Configure power management in Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This article explains how to set up power management in Configuration Manager.

Enable and configure client settings

This procedure configures the *default client settings* for power management. It applies to all the computers in your hierarchy.

If you want to apply these settings to only some computers, create a *custom device client setting*. Then assign it to a collection that contains the computers for power management. For more information, see How to configure client settings.

1. In the Configuration Manager console, go to the **Administration** workspace, select the **Client Settings** node, and select **Default Client Settings**.
2. On the **Home** tab of the ribbon, in the **Properties** group, select **Properties**.
3. Select the **Power Management** group.
4. Enable the client setting to **Allow power management of devices**.
5. Configure the additional client settings that you require. For more information, see About client settings - Power Management.

Clients configure these settings when they next download client policy. To initiate policy retrieval for a single client, see How to manage clients.

Exclude computers

You can prevent collections of computers from receiving power management settings. If a computer is a member of *any* collection that you exclude from power management settings, that computer doesn't apply power management settings. This behavior applies even if it's a member of another collection that does apply power management settings.

You might want to exclude computers from power management for the following reasons:

- You have a business requirement for computers to be turned on at all times.
- You have a control collection of computers on which you don't want to apply power management settings.
- Some of your computers are incapable of applying power management settings.
- You want to exclude computers that run Windows Server from power management.

> **NOTE**
> If you configure the client setting to **Allow users to exclude their device from power management**, users can exclude their own computers from power management by using Software Center.

To find out which computers are excluded from power management, run the report **Computers Excluded**. For more information about this report see How to monitor and plan for power management.

> **IMPORTANT**
>
> Excluding a computer from power management causes all power settings to be reverted to their original values. You cannot revert individual power settings to their original values.

How to exclude a collection of computers from power management

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace, and select the **Device Collections** node.
2. Select the collection that you want to exclude from power management. In the **Home** tab of the ribbon, in the **Properties** group, select **Properties**.
3. Switch to the **Power Management** tab, and select **Never apply power management settings to computers in this collection**.

Next steps

How to create and apply power plans

How to monitor and plan for power management

How to create and apply power plans in System Center Configuration Manager

4/18/2019 • 6 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Power management in System Center Configuration Manager enables you to apply power plans that are supplied with Configuration Manager to collections of computers in your hierarchy, or to create your own custom power plans. Use the procedure in this topic to apply a built-in or custom power plan to computers.

> **IMPORTANT**
> You can only apply Configuration Manager power plans to device collections.

If a computer is a member of multiple collections, each applying different power plans, then the following actions will be taken:

- Power plan: If multiple values for power settings are applied to a computer, the least restrictive value is used.
- Wakeup time: If multiple wakeup times are applied to a desktop computer, the time closest to midnight is used.

  Use the **Computers with Multiple Power Plans** report to display all computers that have multiple power plans applied to them. This can help you discover computers that have power conflicts. For more information about power management reports, see How to monitor and plan for power management in System Center Configuration Manager.

> **IMPORTANT**
> Power settings configured by using Windows Group Policy will override settings configured by Configuration Manager power management.

Use the following procedure to create and apply a Configuration Manager power plan.

To create and apply a power plan

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Device Collections**.
3. In the **Device Collections** list, click the collection to which you want to apply power management settings and then, in the **Home** tab, in the **Properties** group, click **Properties**.
4. In the **Power Management** tab of the <*Collection Name*>**Properties** dialog box, select **Specify power management settings for this collection**.

   > **NOTE**
   > You can also click **Browse** and then copy the power management settings from a selected collection to the selected collection.

5. In the **Start** and **End** fields, specify the start and end time for peak (or business) hours.
6. Enable **Wakeup time (desktop computers)** to specify a time when a desktop computer will wake from sleep or wake from hibernate to install scheduled updates or software installations.

   > **IMPORTANT**
   > Power management uses the internal Windows wakeup time feature to wake computers from sleep or hibernate. Wakeup time settings are not applied to portable computers to prevent scenarios in which they might wake when not plugged in. The wake up time is randomized and computers will be woken over a one hour period from the specified wakeup time.

7. If you want to configure a custom power plan for peak (or business) hours, select **Customized Peak (ConfigMgr)** from the **Peak plan** drop-down list, and then click **Edit**. If you want to configure a power plan for non-peak (or nonbusiness) hours, select **Customized Non-Peak (ConfigMgr)** from the **Non-peak plan** drop-down list, and then click **Edit**.

   > **NOTE**
   > You can use the **Computer Activity** report to help you decide the schedules to use for peak and non-peak hours when you apply power plans to collections of computers. For more information, see How to monitor and plan for power management in System Center Configuration Manager.

   You can also select from the built-in power plans, **Balanced (ConfigMgr)**, **High Performance (ConfigMgr)** and **Power Saver (ConfigMgr)**, and then click **View** to display the properties of each power plan.

   > **NOTE**
   > You cannot modify the built-in power plans.

8. In the <*power plan name*>**Properties** dialog box, configure the following settings:

   - **Name:** Specify a name for this power plan or use the supplied default value.
   - **Description:** Specify a description for this power plan or use the supplied default value.
   - **Specify the properties for this power plan:** Configure the power plan properties. To disable a property, clear its check box. For information about the available settings, see Available power management plan settings in this topic.

     > **IMPORTANT**
     > Enabled settings are applied to computers when the power plan is applied. If you clear a power setting check box, the value on the client computer is not changed when the power plan is applied. Clearing a check box does not restore the power setting to its previous value before a power plan was applied.

9. Click **OK** to close the <*power plan name*>**Properties** dialog box.
10. Click **OK** to close the <*Collection Name*>**Settings** dialog box and to apply the power plan.

Available power management plan settings

The following table lists the power management settings available in Configuration Manager. You can configure

separate settings for when the computer is plugged in or running on battery power. Depending on the version of Windows you are using, some settings might not be configurable.

> **NOTE**
> Power settings that you do not configure will retain their current value on client computers.

NAME	DESCRIPTION
Turn off display after (minutes)	Specifies the length of time, in minutes, that the computer must be inactive before the display is turned off. Specify a value of **0** if you do not want power management to turn off the display.
Sleep after (minutes)	Specifies the length of time, in minutes, that the computer must be inactive before it enters sleep. Specify a value of **0** if you do not want power management to enter sleep on the computer.
Require a password on wakeup	A **Yes** or **No** value specifies whether a password is required to unlock the computer when it enters wake from sleep.
Power button action	Specifies the action that is taken when the computer's power button is pressed. Possible values **Do nothing**, **Sleep**, **Hibernate**, and **Shut down**.
Start menu power button	Specifies the action that occurs when you press the computer's **Start** menu power button. Possible values **Sleep**, **Hibernate**, and **Shut down**.
Sleep button action	Specifies the action that occurs when you press the computer's **Sleep** button. Possible values **Do nothing**, **Sleep**, **Hibernate**, and **Shut down**.
Lid close action	Specifies the action that occurs when the user closes the lid of a portable computer. Possible values **Do nothing**, **Sleep**, **Hibernate**, and **Shut down**.
Turn off hard disk after (minutes)	Specifies the length of time, in minutes, that the computer's hard disk must be inactive before it is turned off. Specify a value of **0** if you do not want power management to turn off the computer's hard disk.
Hibernate after (minutes)	Specifies the length of time, in minutes, that the computer must be inactive before it enters hibernate. Specify a value of **0** if you do not want power management to enter hibernate on the computer.
Low battery action	Specifies the action that occurs when the computer's battery reaches the specified low battery notification level. Possible values **Do nothing**, **Sleep**, **Hibernate**, and **Shut down**.
Critical battery action	Specifies the action that is taken when the computer's battery reaches the specified critical battery notification level. When **On battery** possible values **Sleep**, **Hibernate**, and **Shut down**. When **Plugged in** possible values **Do nothing**, **Sleep**, **Hibernate**, and **Shut down**.

NAME	DESCRIPTION
Allow hybrid sleep	Selecting the **On** or **Off** value specifies whether Windows saves a hibernation file when entering sleep, which can be used to restore the computer's state in the event of power loss while it has entered sleep. Hybrid sleep is designed for desktop computers and, by default, is not enabled on portable computers. On computers that are running Windows 7, enabling hybrid sleep disables the hibernate functionality.
Allow standby state when sleeping action	Selecting the **On** or **Off** value enables the computer to be on standby, which still consumes some power, but enables the computer to wake faster. If this setting is set to **Off**, the computer can only hibernate or turn off.
Required idleness to sleep (%)	Specifies the percentage of idle time on the computer processor time required for the computer to enter sleep. For computers running Windows 7, this value is always set to **0**.
Enable Windows wake up timer for desktop computers	Selecting the **Enable** or **Disable** value can enable the built-in Windows timer to be used by power management to wake a desktop computer. When a desktop computer is woken by using the Windows wake up timer, it will remain awake for 10 minutes by default to allow time for the computer to install any updates or to receive policy. Wakeup timers are not supported on portable computers to prevent scenarios in which they might wake when they are not plugged in.

How to monitor and plan for power management in System Center Configuration Manager

2/12/2019 • 32 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Use the following information to help you monitor and plan for power management in System Center Configuration Manager.

How to use reports for power management

Power management in Configuration Manager includes several reports to help you analyze power consumption and computer power settings in your organization. The reports can also be used to help you troubleshoot problems.

Before you can use the power management reports, you must configure reporting for your hierarchy. For more information about reporting in Configuration Manager, see Reporting in System Center Configuration Manager.

> **NOTE**
>
> Power management information used by daily reports is retained in the Configuration Manager site database for 31 days.
> Power management information used by monthly reports is retained in the Configuration Manager site database for 13 months.
>
> When you run reports during the monitoring and planning and compliance phases of power management, save or export the results from any reports for which you want to retain the data for later comparison in case they are later removed by Configuration Manager.

List of power management reports

The following lists details the power management reports that are available in Configuration Manager.

> **NOTE**
>
> Power management reports display the number of physical computers and the number of virtual computers in a selected collection. However, only power management information from physical computers is displayed in power management reports.

Computer Activity report

The **Computer Activity** report displays a graph showing the following activity for a specified collection over a specified period:

- **Computer On** – The computer has been turned on.
- **Monitor On** – The monitor has been turned on.
- **User Active** – Activity has been detected from the computer mouse, computer keyboard, or from a Remote Desktop connection to the computer

This report is used during the monitoring and planning and enforcement stages to help you understand the alignment between computer activity, monitor activity and user activity over a 24 hour period. If you run the report over a number of days then the data is aggregated over this period. This report can help you to determine typical business (peak) and nonbusiness (non-peak) hours for a selected collection to help you decide when to apply configured power management plans.

The graph shows time periods where a computer might be turned on, but there is no user activity. Consider applying more restrictive power settings during these times to save on the power costs of computers that are turned on, but are not being used. A computer is counted as being active if there has been computer, user or monitor activity for one minute or more for a displayed hour on the graph. If a computer is not reporting power management data, it will not be included in the **Computer Activity** report.

Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Start date	From the drop-down list, select the start date for this report.
End date (Optional)	From the drop-down list, select an optional end date for this report.
Collection name	From the drop-down list, select a collection to use for this report.
Device type	From the drop-down list, select the type of computer for which you want a report. Valid values are **All** (both desktop and portable computers), **Desktop** (desktop computers only), and **Laptop** (portable computers only).

Hidden report parameters

This report has no hidden parameters that you can set.

Report links

If a value for **End date (optional)** is not specified, this report contains a link to the following report which provides further information.

REPORT NAME	DETAILS
Computer Activity Details	Click the **Click for detailed information** link to see a list of active, inactive and non-reporting computers for the specified date. For more information, see Computer Activity Details Report in this topic.

Computer Activity by Computer report

The **Computer Activity by Computer** report displays a graph showing the following activity for a specified computer on a specified date:

- **Computer On** – The computer has been turned on.
- **Monitor On** – The monitor has been turned on.

- **User Active** – Activity has been detected from the computer mouse, computer keyboard, or from a Remote Desktop connection to the computer.

  This report can be run independently or called by the **Computer Activity Details** report.

> **NOTE**
> Information about computer activity is collected from client computers during hardware inventory. Depending on the time at which hardware inventory runs, activity during an applied peak or non-peak power plan might be collected.

Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Report date	From the drop-down list, select a date for this report.
Computer name	Enter a computer name for which you want a report.

Hidden report parameters

This report has no hidden parameters that you can set.

Report links

This report contains links to the following report which provides further information about the selected item.

REPORT NAME	DETAILS
Computer Details	Click the **Click for detailed information** link to see the power capabilities, power settings, and applied power plans for the selected computer.

Computer Activity Details report

The **Computer Activity Details** report displays a list of active or inactive computers with their sleep and wake capabilities. This report is called by the Computer Activity Report and is not designed to be run directly by the site administrator.

Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Collection name	From the drop-down list, select a collection to use for this report.
Report date	From the drop-down list, select a date to use for this report.
Report hour	From the drop-down list, select an hour from the specified date for which to run this report. Valid values are between **12am** and **11pm**.

PARAMETER NAME	DESCRIPTION
Computer state	From the drop-down list, select the computer state for which to run this report. Valid values are **All** (computers that were turned on or off), **On** (computers that were turned on), and **Off** (computers that were turned off, in sleep, or in hibernate). These values are only returned for the chosen reporting period.
Device type	From the drop-down list, select the type of computer for which you want a report. Valid values are **All** (both desktop and portable computers), **Desktop** (desktop computers only), and **Laptop** (portable computers only). These values are only returned for the chosen reporting period.
Sleep capable	From the drop-down list, select if you want to display computers capable of sleep in the report. Valid values are **All** (both computers capable and incapable of sleep), **No** (computers that are incapable of sleep), and **Yes** (computers that are capable of sleep).
Wake from sleep capable	From the drop-down list, select if you want to display computers capable of wake from sleep in the report. Valid values are **All** (both computers capable and incapable of wake from sleep), **No** (computers that are incapable of wake from sleep), and **Yes** (computers that are capable of wake from sleep).
Power plan	From the drop-down list, select the power plan types you want to display in the report. Valid values are **All** (computers that do not have any power management plans applied; computers that have a power management plan applied; computers excluded from power management), **Not specified** (computers that do not have a power management plan applied), **Defined** (computers that have a power management plan applied), and **Excluded** (computers that have been excluded from power management).
Operating system	From the drop-down list, select the computer operating systems that you want to display in the report or select **All** to display all operating systems.

Hidden report parameters

This report has no hidden parameters that you can set.

Report links

This report contains links to the following report which provides further information about the selected item.

REPORT NAME	DETAILS
Computer Activity by Computer	Click a computer name to see specific activity for that computer over a chosen reporting period. These activities include **Computer on** (has the computer been turned on?), **Monitor on** (has the monitor been turned on?), and **User Active** (activity has been detected from the computer's mouse, keyboard, or a remote desktop connection). For more information, see Computer Activity by Computer Report in this topic.

Computer Details report

The **Computer Details** report displays detailed information about the power capabilities, power settings, and power plans applied to a specified computer. This report is called by the **Computer Activity by Computer** report, the **Computers with Multiple Power Plans** report, the **Power Capabilities** report and the **Power Settings Details** report. It is not designed to be run directly by the site administrator.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Computer name	Enter a computer name for which you want a report.
Power mode	From the drop down list, select the type of power settings you want to display in the report results. Select **Plugged In** to view the power settings configured for when the computer is plugged in and **On Battery** to view the power settings configured for when the computer is running on battery power.

Hidden report parameters

This report has no hidden parameters you can set.

Report links

This report does not link to any other power management reports.

Computer Not Reporting Details report

The **Computer Not Reporting Details** report displays a list of computers in a specified collection that have not reported any power activity on a specified date and time. This report is called by the **Computer Activity Report** and is not designed to be run directly by the site administrator.

> **NOTE**
> Computers report power management information as part of their hardware inventory schedule. Before you consider a computer to not be reporting, ensure it has reported hardware inventory.

Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Collection name	From the drop-down list, select a collection to use for this report.
Report date	From the drop-down list, select a date for this report.
Report hour	From the drop-down list, select an hour from the specified date for which to run this report. Valid values are between **12am** and **11pm**.

PARAMETER NAME	DESCRIPTION
Device type	From the drop-down list, select the type of computer for which you want a report. Valid values are **All** (both desktop and portable computers), **Desktop** (desktop computers only), and **Laptop** (portable computers only). These values are only returned for the chosen reporting period.

Hidden report parameters

This report has no hidden parameters that you can set.

Report links

This report does not link to any other power management reports.

Computers Excluded

The **Computers Excluded** report displays a list of computers in a specified collection that have been excluded from Configuration Manager power management.

Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Collection	From the drop-down list, select a collection for this report.
Reason	From the drop-down list, select the reason why the computers were excluded from power management. You can display **All** (all excluded computers), **Excluded by administrator** (only computers that were excluded by an administrative user), and **Excluded by user** (only computers that were excluded by a user of Software Center).

Hidden report parameters

This report has no hidden parameters that you can set.

Report links

This report contains links to the following report which provides further information about the selected item.

REPORT NAME	DETAILS
Power Computer Details	Click a computer name to see the power capabilities, power settings, and applied power plans for the selected computer. For more information, see Computer Details Report in this topic.

Computers with Multiple Power Plans

The **Computers with Multiple Power Plans** report displays a list of computers that are members of multiple collections, each applying different power plans. For each computer with potentially conflicting power settings, the report displays the computer name and the power plans being applied for each collection that the computer is a member of.

IMPORTANT

If a computer is a member of multiple collections, where each collection has different power plans, then the least restrictive power plan will be applied.

If a computer is a member of multiple collections, where each collection has different wakeup times, then the time closest to midnight will be used.

Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Collection name	From the drop-down list, select a collection for this report.

Hidden report parameters

This report has no hidden parameters that you can set.

Report links

This report contains links to the following report which provides further information about the selected item.

REPORT NAME	DETAILS
Power Computer Details	Click a computer name to see the power capabilities, power settings, and applied power plans for the selected computer. For more information, see Computer Details Report in this topic.

Energy Consumption report

The **Energy Consumption** report displays the following information:

- A graph showing the total monthly power consumption of computers in kiloWatt per hour (kWh) in the specified collection for the specified time period.
- A graph showing the average power consumption in kiloWatt per hour (kWh) of each computer in the specified collection for the specified time period.
- A table showing the total monthly power consumption in kiloWatt per hour (kWh) and the average power consumption of computers in the specified collection for the specified time period.

  This information can be used to help you to understand power consumption trends in your environment. After applying a power plan to computers in the selected collection, the power consumption of computers should decrease.

NOTE

If you add or remove members to the collection after you have applied a power plan, this will affect the results shown by the **Energy Consumption** report and might make it more difficult to compare the results from the monitoring and planning phase and the enforcement phase.

Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Start date	From the drop-down list, select a start date for this report.
End date	From the drop-down list, select an end date for this report.
Collection name	From the drop-down list, select a collection for this report.
Device type	From the drop-down list, select the type of computer for which you want a report. Valid values are **All** (both desktop and portable computers), **Desktop** (desktop computers only), and **Laptop** (portable computers only). These values are only returned for the chosen reporting period.

Hidden report parameters

The following hidden parameters can optionally be specified to change the behavior of this report.

PARAMETER NAME	DESCRIPTION
Desktop computer on	Specify the power consumption of a desktop computer when it is turned on. The default value is **0.07** kW per hour.
Laptop computer on	Specify the power consumption of a portable computer when it is turned on. The default value is **0.02** kW per hour.
Desktop computer sleep	Specify the power consumption of a desktop computer that has entered sleep. The default value is **0.003** kW per hour.
Laptop computer sleep	Specify the power consumption of a portable computer that has entered sleep. The default value is **0.001** kW per hour.
Desktop computer off	Specify the power consumption of a desktop computer when it is turned off. The default value is **0** kW per hour.
Laptop computer off	Specify the power consumption of a portable computer when it is turned off. The default value is **0** kW per hour.
Desktop monitor on	Specify the power consumption of a desktop computer monitor when it is turned on. The default value is **0.028** kW per hour.
Laptop monitor on	Specify the power consumption of a portable computer monitor when it is turned on. The default value is **0** kW per hour.

Report links

This report does not link to any other power management reports.

Energy Consumption by Day report

The **Energy Consumption by Day** report displays the following information:

- A graph showing the total daily power consumption of computers in kiloWatt per hour (kWh) in the specified collection for the last 31 days.
- A graph showing the average daily power consumption in kiloWatt per hour (kWh) of each computer in the specified collection for last 31 days.

- A table showing the total daily power consumption in kiloWatt per hour (kWh) and the average daily power consumption of computers in the specified collection for the last 31 days.

  This information can be used to help you to understand power consumption trends in your environment. After applying a power plan to computers in the selected collection, the power consumption of computers should decrease.

> **NOTE**
> If you add or remove members to the collection after you have applied a power plan, this will affect the results shown by the **Energy Consumption** report and might make it more difficult to compare the results from the monitoring and planning phase and the enforcement phase.

Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Collection	From the drop-down list, select a collection for this report.
Device Type	From the drop-down list, select the type of computer for which you want to report. Valid values are **All** (both desktop and portable computers), **Desktop** (desktop computers only), and **Laptop** (portable computers only). These values are only returned for the chosen reporting period.

Hidden report parameters

The following hidden parameters can optionally be specified to change the behavior of this report.

PARAMETER NAME	DESCRIPTION
Desktop computer on	Specify the power consumption of a desktop computer when it is turned on. The default value is **0.07** kW per hour.
Laptop computer on	Specify the power consumption of a portable computer when it is turned on. The default value is **0.02** kW per hour.
Desktop computer sleep	Specify the power consumption of a desktop computer that has entered sleep. The default value is **0.003** kW per hour.
Laptop computer sleep	Specify the power consumption of a portable computer that has entered sleep. The default value is **0.001** kW per hour.
Desktop computer off	Specify the power consumption of a desktop computer when it is turned off. The default value is **0** kW per hour.
Laptop computer off	Specify the power consumption of a portable computer when it is turned off. The default value is **0** kW per hour.
Desktop monitor on	Specify the power consumption of a desktop computer monitor when it is turned on. The default value is **0.028** kW per hour.

PARAMETER NAME	DESCRIPTION
Laptop monitor on	Specify the power consumption of a portable computer monitor when it is turned on. The default value is **0** kW per hour.

Report links

This report does not link to any other power management reports.

Energy Cost report

The **Energy Cost** report displays the following information:

- A graph showing the total monthly power cost for computers in the specified collection for specified time period.
- A graph showing the average monthly power cost for each computer in the specified collection for the specified time period.
- A table showing the total monthly power cost and the average monthly power cost for computers in the specified collection for the last 31 days.

  This information can be used to help you to understand power cost trends in your environment. After applying a power plan to computers in the selected collection, the power cost for computers should decrease.

  Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Start date	From the drop-down list, select a start date for this report.
End date	From the drop-down list, select an end date for this report.
Cost of KwH	Specify the cost per kWh of electricity. The default value is **0.09**. You can modify the unit of currency used by this report in the hidden parameters section.
Collection name	From the drop-down list, select a collection to use for this report.
Device type	From the drop-down list, select the type of computer for which you want to report. Valid values are **All** (both desktop and portable computers), **Desktop** (desktop computers only), and **Laptop** (portable computers only). These values are only returned for the chosen reporting period.

Hidden report parameters

The following hidden parameters can optionally be specified to change the behavior of this report.

PARAMETER NAME	DESCRIPTION

PARAMETER NAME	DESCRIPTION
Desktop computer on	Specify the power consumption of a desktop computer when it is turned on. The default value is **0.07** kW per hour.
Laptop computer on	Specify the power consumption of a portable computer when it is turned on. The default value is **0.02** kW per hour.
Desktop computer sleep	Specify the power consumption of a desktop computer that has entered sleep. The default value is **0.003** kW per hour.
Laptop computer sleep	Specify the power consumption of a portable computer that has entered sleep. The default value is **0.001** kW per hour.
Desktop computer off	Specify the power consumption of a desktop computer when it is turned off. The default value is **0** kW per hour.
Laptop computer off	Specify the power consumption of a portable computer when it is turned off. The default value is **0** kW per hour.
Desktop monitor on	Specify the power consumption of a desktop computer monitor when it is turned on. The default value is **0.028** kW per hour.
Laptop monitor on	Specify the power consumption of a portable computer monitor when it is turned on. The default value is **0** kW per hour.
Currency	Specify the currency label to use for this report. The default value is **USD ($)**.

Report links

This report does not link to any other power management reports.

Energy Cost by Day report

The **Energy Cost by Day** report displays the following information:

- A graph showing the total daily power cost for computers in the specified collection for the last 31 days.
- A graph showing the average daily power cost for each computer in the specified collection for the last 31 days.
- A table showing the total daily power cost and the average daily power cost for computers in the specified collection for the last 31 days.

  This information can be used to help you to understand power cost trends in your environment. After applying a power plan to computers in the selected collection, the power cost for computers should decrease.

  Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION

PARAMETER NAME	DESCRIPTION
Collection name	From the drop-down list, select a collection to use for this report.
Device type	From the drop-down list, select the type of computer you want to report about. Valid values are **All** (both desktop and portable computers), **Desktop** (desktop computers only), and **Laptop** (portable computers only). These values are only returned for the chosen reporting period.
Cost of KwH	Specify the cost per kWh of electricity. The default value is **0.09**. You can modify the unit of currency used by this report in the hidden parameters section.

Hidden report parameters

The following hidden parameters can optionally be specified to change the behavior of this report.

PARAMETER NAME	DESCRIPTION
Desktop computer on	Specify the power consumption of a desktop computer when it is turned on. The default value is **0.07** kW per hour.
Laptop computer on	Specify the power consumption of a portable computer when it is turned on. The default value is **0.02** kW per hour.
Desktop computer sleep	Specify the power consumption of a desktop computer that has entered sleep. The default value is **0.003** kW per hour.
Laptop computer sleep	Specify the power consumption of a portable computer that has entered sleep. The default value is **0.001** kW per hour.
Desktop computer off	Specify the power consumption of a desktop computer when it is turned off. The default value is **0** kW per hour.
Laptop computer off	Specify the power consumption of a portable computer when it is turned off. The default value is **0** kW per hour.
Desktop monitor on	Specify the power consumption of a desktop computer monitor when it is turned on. The default value is **0.028** kW per hour.
Laptop monitor on	Specify the power consumption of a portable computer monitor when it is turned on. The default value is **0** kW per hour.
Currency	Specify the currency label to use for this report. The default value is **USD ($)**.

Report links

This report does not link to any other power management reports.

Environmental Impact report

The **Environmental Impact** report displays the following information:

- A graph showing the total monthly CO2 generated (in tons) for computers in the specified collection for the specified time period.
- A graph showing the average monthly CO2 generated (in tons) for each computer in the specified collection for the specified time period.
- A table showing the total monthly CO2 generated and the average monthly CO2 generated for computers in the specified collection for specified time period.

  The **Environmental Impact** report calculates the amount of CO2 generated (in tons) by using the time that a computer or monitor was turned on in a 24 hour period.

  Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Report start date	From the drop-down list, select a start date for this report.
Report end date	From the drop-down list, select an end date for this report.
Collection name	From the drop-down list, select a collection for this report.
Device type	From the drop-down list, select the type of computer for which you want a report. Valid values are **All** (both desktop and portable computers), **Desktop** (desktop computers only), and **Laptop** (portable computers only). These values are only returned for the chosen reporting period.

Hidden report parameters

The following hidden parameters can optionally be specified to change the behavior of this report.

PARAMETER NAME	DESCRIPTION
Desktop computer on	Specify the power consumption of a desktop computer when it is turned on. The default value is **0.07** kW per hour.
Laptop computer on	Specify the power consumption of a portable computer when it is turned on. The default value is **0.02** kW per hour.
Desktop computer sleep	Specify the power consumption of a desktop computer that has entered sleep. The default value is **0.003** kW per hour.
Laptop computer sleep	Specify the power consumption of a portable computer that has entered sleep. The default value is **0.001** kW per hour.
Desktop computer off	Specify the power consumption of a desktop computer when it is turned off. The default value is **0** kW per hour.
Laptop computer off	Specify the power consumption of a portable computer when it is turned off. The default value is **0** kW per hour.
Desktop monitor on	Specify the power consumption of a desktop computer monitor when it is turned on. The default value is **0.028** kW per hour.

PARAMETER NAME	DESCRIPTION
Laptop monitor on	Specify the power consumption of a portable computer monitor when it is turned on. The default value is **0** kW per hour.
Carbon Factor (tons/kWh) (CO2Mix)	Specify the value for carbon factor (in tons/kWh) that you typically can obtain from your power company. The default value is **0.0015** tons per kWh.

Report links

This report does not link to any other power management reports.

Environmental Impact by Day report

The **Environmental Impact by Day** report displays the following information:

- A graph showing the total daily CO2 generated (in tons) for computers in the specified collection for the last 31 days.
- A graph showing the average daily CO2 generated (in tons) for each computer in the specified collection for the last 31 days.
- A table showing the total daily CO2 generated and the average daily CO2 generatedfor computers in the specified collection for the last 31 days.

  The **Environmental Impact by Day** report calculates the amount of CO2 generated (in tons) by using the time that a computer or monitor was turned on in a 24 hour period.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Collection name	From the drop-down list, select a collection for this report.
Device type	From the drop-down list, select the type of computer you want to report about. Valid values are **All** (both desktop and portable computers), **Desktop** (desktop computers only), and **Laptop** (portable computers only). These values are only returned for the chosen reporting period.

Hidden report parameters

The following hidden parameters can optionally be specified to change the behavior of this report.

PARAMETER NAME	DESCRIPTION
Desktop computer on	Specify the power consumption of a desktop computer when it is turned on. The default value is **0.07** kWh.
Laptop computer on	Specify the power consumption of a portable computer when it is turned on. The default value is **0.02** kWh.
Desktop computer off	Specify the power consumption of a desktop computer when it is turned off. The default value is **0** kWh.
Laptop computer off	Specify the power consumption of a portable computer when it is turned off. The default value is **0** kWh.

PARAMETER NAME	DESCRIPTION
Desktop computer sleep	Specify the power consumption of a desktop computer that has entered sleep. The default value is **0.003** kWh.
Laptop computer sleep	Specify the power consumption of a portable computer has entered sleep. The default value is **0.001** kWh.
Desktop monitor on	Specify the power consumption of a desktop computer monitor when it is turned on. The default value is **0.028** kWh.
Laptop monitor on	Specify the power consumption of a portable computer monitor when it is turned on. The default value is **0** kWh.
Carbon Factor (tons/kWh) (CO2Mix)	Specify a value for the carbon factor (in tons/kWh) that you typically can obtain from your power company. The default value is **0.0015** tons per kWh.

Report links

This report does not link to any other power management reports.

Insomnia Computer Details report

The **Insomnia Computer Details** report displays a list of computers that did not sleep or hibernate for a specific reason within a specified time period. This report is called by the **Insomnia Report** and is not designed to be run directly by the site administrator.

The **Insomnia Report** displays computers as **Not sleep capable** when they are not capable of sleep and have been turned on during the entire specified report interval. The report displays computers as **Not hibernate capable** when they are not capable of hibernate and have been turned on during the entire specified report interval.

> **NOTE**
> Power management can only collect causes that prevented computers from entering sleep or hibernate from computers running Windows 7 or Windows Server 2008 R2.

Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Collection name	From the drop-down list, select a collection to use for this report.
Report interval (days)	Specify the number of days to report. The default value is **7** days.
Cause of Insomnia	From the drop-down list, select one of the causes that can prevent computers from entering sleep or hibernate.

Hidden report parameters

This report has no hidden parameters that you can set.

Report links

This report contains links to the following report which provides further information about the selected item.

REPORT NAME	DETAILS
Computer Details	Click the **Click for detailed information** link to see the power capabilities, power settings, and applied power plans for the selected computer. For more information, see Computer Details Report in this topic.

Insomnia report

The **Insomnia Report** displays a list of common causes that prevented computers from entering sleep or hibernate and the number of computers affected by each cause for a specified time period. There are a number of causes that might prevent a computer from entering sleep or hibernate such as a process running on the computer, an open Remote Desktop session, or that the computer is incapable of sleep or hibernate. From this report, you can open the **Insomnia Computer Details** report which displays a list of computers affected by each cause of computers not sleeping or hibernating.

The Power Insomnia report displays computers as **Not sleep capable** when they are not capable of sleep and have been turned on during the entire specified report interval. The report displays computers as **Not hibernate capable** when they are not capable of hibernate and have been turned on during the entire specified report interval.

> **NOTE**
> Power management can only collect causes that prevented computers from entering sleep or hibernate from computers running Windows 7 or Windows Server 2008 R2.

Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Collection name	From the drop-down list, select a collection to use for this report.
Report interval (days)	Specify the number of days to report. The default value is **7** days. The maximum value is **365** days. Specify **0** to run the report for today.

Hidden report parameters

This report has no hidden parameters that you can set.

Report links

This report contains links to the following report which provides further information about the selected item.

REPORT NAME	DETAILS

REPORT NAME	DETAILS
Insomnia Computer Details	Click a number in the **Affected Computers** column to see a list of computers that could not sleep or hibernate because of the selected cause. For more information, see Insomnia Computer Details Report in this topic.

Power Capabilities report

The **Power Capabilities** report displays the power management hardware capabilities of computers in the specified collection. This report is typically used in the monitoring phase of power management to determine the power management capabilities of computers in your organization. The information displayed in the report can then be used to create collections of computers to apply power plans to, or to exclude from power management. The power management capabilities displayed by this report are:

- **Sleep Capable** - Indicates whether the computer has the capability to enter sleep if it is configured to do so.
- **Hibernate Capable** – Indicates whether the computer can enter hibernate if it is configured to do so.
- **Wake from Sleep** – Indicates whether the computer can wake from sleep if it is configured to do so.
- **Wake from Hibernate** – Indicates whether the computer can wake from hibernate if it is configured to do so.

  The values reported by the **Power Capabilities** report indicate the sleep and hibernate capabilities of computers as reported by Windows. However, the reported values do not reflect cases where Windows or BIOS settings prevent these functions from working.

  Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Collection	From the drop-down list, select a collection for this report.
Display Filter	From the drop-down list, select **Not Supported** to display only computers in the specified collection that are incapable of sleep, hibernate, wake from sleep, or wake from hibernate. Select **Show All** to display all computers in the specified collection.

Hidden report parameters

This report has no hidden parameters that you can set.

Report links

This report contains links to the following report which provides further information about the selected item.

REPORT NAME	DETAILS
Computer Details	Click a computer name to see the power capabilities, power settings, and applied power plans for the selected computer. For more information, see Computer Details Report in this topic.

Power Settings report

The **Power Settings** report displays an aggregated list of power settings used by computers in the specified collection. For each power setting, the possible power modes, values, and units are displayed, together with a count of the number of computers that use those values. This report can be used during the monitoring phase of power management to help the administrator understand the existing power settings used by computers in the site and to help plan optimal power settings to be applied by using a power management plan. The report is also useful when troubleshooting to validate that power settings were correctly applied.

> **NOTE**
> The settings displayed are collected from client computers during hardware inventory. Depending on the time at which hardware inventory runs, settings from applied peak or non-peak power plans might be collected.

Use the following parameters to configure this report.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Collection name	From the drop-down list, select a collection for this report.

Hidden report parameters

The following hidden parameters can optionally be specified to change the behavior of this report.

PARAMETER NAME	DESCRIPTION
numberOfLocalizations	Specify the number of languages in which you want to view power setting names reported by client computers. If you only want to view the most popular language, leave this setting at the default of **1**. To view all languages, set this value to **0**.

Report links

This report contains links to the following report which provides further information about the selected item.

REPORT NAME	DETAILS
Power Settings Details	Click the number of computers in the **Computers** column to see a list of all computers that use the power settings in that row. For more information, see Power Settings Details Report in this topic.

Power Settings Details report

The **Power Settings Details** report displays further information about computers selected in the **Power Settings** report. This report is called by the **Power Settings** report and is not designed to be run directly by the site administrator.

Required report parameters

The following parameters must be specified to run this report.

PARAMETER NAME	DESCRIPTION
Collection	From the drop-down list, select a collection to use for this report.
Power Setting GUID	From the drop-down list, select the power setting GUID on which you want to report. For a list of all power settings and their uses, see Available power management plan settings in the topic How to create and apply power plans in System Center Configuration Manager.
Power Mode	From the drop down list, select the type of power settings you want to display in the report results. Select **Plugged In** to view the power settings configured for when the computer is plugged in and **On Battery** to view the power settings configured for when the computer is running on battery power.
Setting Index	From the drop-down list, select the value for the selected power setting name on which you want to report. For example, if you want to display all computers with the **turn off hard disk after** setting set to **10** minutes, select **turn off hard disk after** for **Power Setting Name** and **10** for **Setting Index**.

Hidden report parameters

The following hidden parameters can optionally be specified to change the behavior of this report.

PARAMETER NAME	DESCRIPTION
numberOfLocalizations	Specify the number of languages in which you want to view power setting names reported by client computers. If you only want to view the most popular language, leave this setting at the default of **1**. To view all languages, set this value to **0**.

Report links

This report contains links to the following report which provides further information about the selected item.

REPORT NAME	DETAILS
Computer Details	Click a computer name to see the power capabilities, power settings, and applied power plans for the selected computer. For more information, see Computer Details Report in this topic.

Security and privacy for power management in System Center Configuration Manager

2/12/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

This section contains security and privacy information for power management in System Center Configuration Manager.

Security best practices for power management

There are no security-related best practices for power management.

Privacy information for power management

Power management uses features that are built into Windows to monitor power usage and to apply power settings to computers during business hours and nonbusiness hours. Configuration Manager collects power usage information from computers, which includes data about when a user is using a computer. Although Configuration Manager monitors power usage for a collection rather than for each computer, a collection can contain just one computer. Power management is not enabled by default and must be configured by an administrator.

The power usage information is stored in the Configuration Manager database and is not sent to Microsoft. Detailed information is retained in the database for 31 days and summarized information is retained for 13 months. You cannot configure the deletion interval.

Before you configure power management, consider your privacy requirements.

Upgrade clients in Configuration Manager

9/11/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can use different methods to upgrade the System Center Configuration Manager client software on Windows computers, UNIX and Linux servers, and Mac computers. Here are the advantages and disadvantages of each method.

> **TIP**
> If you are upgrading your server infrastructure from a previous version of Configuration Manager (such as Configuration Manager 2007 or System Center 2012 Configuration Manager), we recommend that you complete the server upgrades including installing all current branch updates, before upgrading the Configuration Manager clients. This way, you'll also have the most recent version of the client software.

Group Policy installation

Supported client platform: Windows

Advantages

- Does not require computers to be discovered before the client can be upgraded.
- Can be used for new client installations or for upgrades.
- Computers can read client installation properties that have been published to Active Directory Domain Services.
- Does not require you to configure and maintain an installation account for the intended client computer.

Disadvantages

- Can cause high network traffic if you're upgrading a lot of clients.
- If the Active Directory schema is not extended for Configuration Manager, you must use Group Policy settings to add client installation properties to computers in your site.

Logon script installation

Supported client platform: Windows

Advantages

- Does not require computers to be discovered before the client can be installed.
- Can be used for new client installations or for upgrades.
- Supports using command-line properties for CCMSetup.

Disadvantages

- Can cause high network traffic if you're upgrading a lot of clients in a short time.
- Can take a long time to upgrade all client computers if users do not frequently log on to the network.

  For more information, see How to Install Configuration Manager Clients by Using Logon Scripts.

Manual installation

Supported client platform: Windows, UNIX/Linus, Mac OS X

Advantages

- Does not require computers to be discovered before the client can be upgraded.
- Can be useful for testing purposes.
- Supports using command-line properties for CCMSetup.

Disadvantages

- No automation, therefore time consuming.

For more information, see the following topics:

- How to Install Configuration Manager Clients Manually
- How to upgrade clients for Linux and UNIX servers in System Center Configuration Manager
- How to upgrade clients on Mac computers in System Center Configuration Manager

Upgrade installation (application management)

Supported client platform: Windows

> **NOTE**
> You cannot upgrade Configuration Manager 2007 clients with this method. In this scenario, you can deploy the Configuration Manager client as a package from the Configuration Manager 2007 site, or you can use automatic client upgrade which automatically creates and deploys a package that contains the latest version of the client.

Advantages

- Supports using command-line properties for CCMSetup.

Disadvantages

- Can cause high network traffic if you distribute the client to large collections.
- Can only be used to upgrade the client software on computers that have been discovered and assigned to the site.

For more information, see How to Install Configuration Manager Clients by Using a Package and Program.

Automatic client upgrade

> **NOTE**
> Can be used to upgrade Configuration Manager 2007 clients to System Center Configuration Manager clients. A Configuration Manager 2007 client can assign to a Configuration Manager site, but cannot perform any actions besides automatic client upgrade.

Supported client platform: Windows

Advantages

- Because of the randomization over the specified period, only auto-upgrade is suitable for large-scale client upgrades. Other methods are either too slow on large scale, or don't have randomization.

> **NOTE**
> Client piloting isn't good for large scale as it doesn't randomize at all.

- Can be used to automatically keep clients in your site at the latest version.
- Requires minimal administration.

Disadvantages

- Can only be used to upgrade the client software and cannot be used to install a new client.
- Applies to all clients in the hierarchy that are assigned to a site. Cannot be scoped by collection.
- Limited scheduling options.

For more information, see How to upgrade clients for Windows computers in System Center Configuration Manager.

Client testing

Supported client platform: Windows

Advantages

- Can be used to test new client versions in a smaller pre-production collection.
- When testing is complete, clients in pre-production are promoted to production and automatically upgraded across the Configuration Manager site.

Disadvantages

- Can only be used to upgrade the client software and cannot be used to install a new client.

How to test client upgrades in a pre-production collection in System Center Configuration Manager

How to test client upgrades in a pre-production collection in System Center Configuration Manager

2/12/2019 • 3 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can test a new Configuration Manager client version in a pre-production collection before upgrading the rest of the site with it. When you do this, only devices that are part of the test collection are upgraded. Once you've had a chance to test the client you can promote the client, which makes the new version of the client software available to the rest of the site.

> **NOTE**
> To promote a test client to production, you must be logged in as a user with security role of **full administrator** and a security scope of **All**. For more information, see Fundamentals of role-based administration. You must also be logged into a server connected to the central administration site or a top-level standalone primary site.

There are 3 basic steps to testing clients in pre-production.

1. Configure automatic client upgrades to use a pre-production collection.
2. Install a Configuration Manager update that includes a new version of the client.
3. Promote the new client to production.

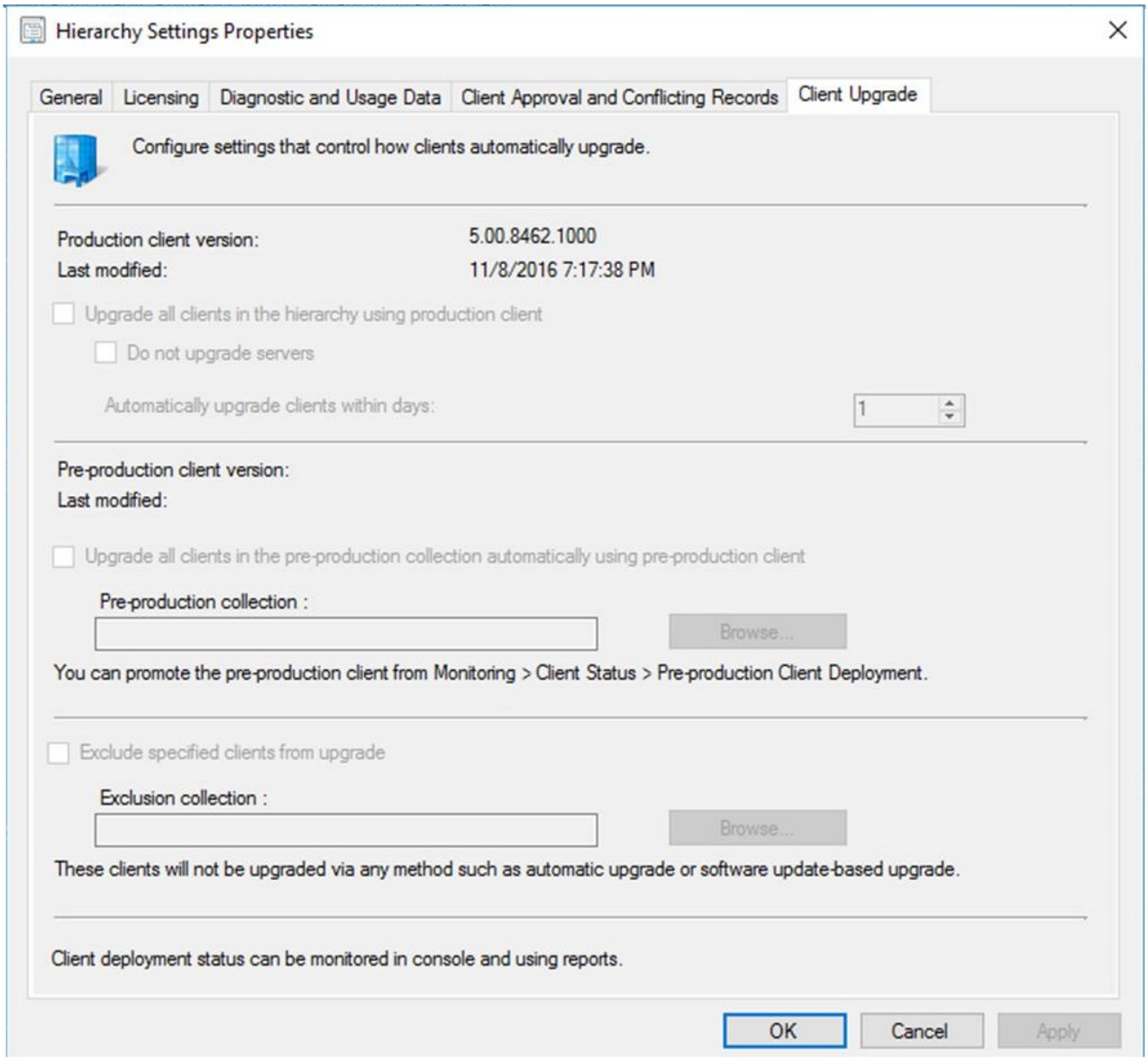
To configure automatic client upgrades to use a pre-production collection

> **IMPORTANT**
> Pre-production client deployment is not supported for workgroup computers. They can't use the authentication required for the distribution point to access the pre-production client package. They will receive the latest client when it is promoted to be the production client.

1. Set up a collection that contains the computers you want to deploy the pre-production client to.
2. In the Configuration Manager console open **Administration** > **Site Configuration** > **Sites**, and choose **Hierarchy Settings**.

   On the **Client Upgrade** tab of the **Hierarchy Settings Properties**:

   - Select **Upgrade all clients in the pre-production collection automatically using pre-production client**
   - Enter the name of a collection to use as a pre-production collection



NOTE

To change these settings, your account must be a member of the **Full Administrator** security role, and the **All** security scope.

To install a Configuration Manager update that includes a new version of the client

1. In the Configuration Manager console, open **Administration** > **Updates and Servicing**, select an **Available** update, and then choose **Install Update Pack**. (Prior to version 1702, Updates and Servicing was under **Administration** > **Cloud Services**.)

   For more information on installing updates, see Updates for System Center Configuration Manager

2. During installation of the update, on the **Client Options** page of the wizard, select **Test in pre-production collection**.

3. Complete the rest of the wizard and install the update pack.

   After the wizard complete, clients in the pre-production collection will begin to deploy the updated client. You can monitor the deployment of upgraded clients by going to **Monitoring** > **Client Status** > **Pre-production Client Deployment**. For more information, see How to monitor client deployment status in System Center Configuration Manager.

> **NOTE**
>
> The deployment status on computers hosting site system roles in a pre-production collection may be reported as **Not compliant** even when the client was successfully deployed. When you promote the client to production, the deployment status is reported correctly.

To promote the new client to production

1. In the Configuration Manager console, open **Administration** > **Updates and Servicing**, and choose **Promote Pre-production Client**. (Prior to version 1702, Updates and Servicing was under **Administration** > **Cloud Services**.)

   > **TIP**
   >
   > The **Promote Pre-production Client** button is also available when you're monitoring client deployments in the console at **Monitoring** > **Client Status** > **Pre-production Client Deployment**.

2. Review the client versions in production and pre-production, make sure the correct the pre-production collection is specified, and then click **Promote**, then **Yes**.

3. After the dialog box closes, the updated client version will replace the client version in use in your hierarchy. You can then upgrade the clients for your whole site. See How to upgrade clients for Windows computers in System Center Configuration Manager for more information.

> **NOTE**
>
> To enable the pre-production client, or to promote a pre-production client to a production client, your account must be a member of a security role that has **Read** and **Modify** permissions for the **Update Packages** object. Client upgrades honor any Configuration Manager maintenance windows you have configured.

How to exclude clients from upgrade in Configuration Manager

8/28/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

You can exclude a collection of clients from automatically installing updated client versions. Use this exclusion for a collection of computers that need greater care when upgrading the client. A client that's in an excluded collection ignores requests to install updated client software.

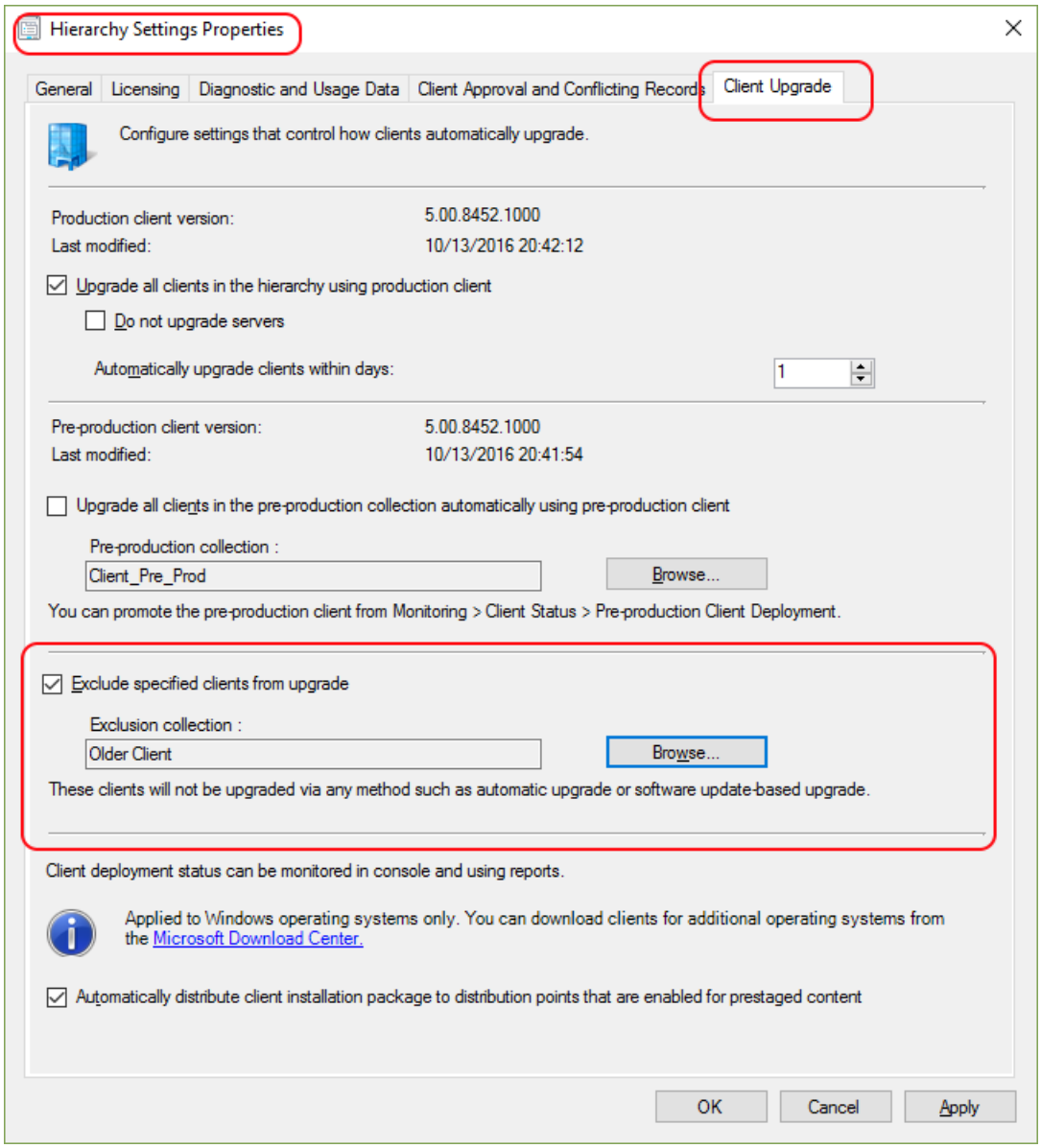
This exclusion applies to the following methods:

- Automatic upgrade
- Software update-based upgrade
- Logon scripts
- Group policy

> **NOTE**
> Although the user interface states that clients won't upgrade via any method, there are two methods you can use to override these settings. Use client push or manual client installation to override this configuration. For more information, see How to upgrade an excluded client.

Configure exclusion

1. In the Configuration Manager console, go to the **Administration** workspace. Expand **Site Configuration**, select the **Sites** node, and then select **Hierarchy Settings** in the ribbon.
2. Switch to the **Client Upgrade** tab.
3. Select the option to **Exclude specified clients from upgrade**. Then select the **Exclusion collection** you want to exclude. You can only select a single collection for exclusion.
4. Select **OK** to close and save the configuration.



After clients in the excluded collection update policy, they don't automatically install client updates. For more information, see How to upgrade clients for Windows computers.

> **NOTE**
> Excluded clients still download and run Ccmsetup, but don't upgrade.

When you remove a client from the exclude collection, it doesn't automatically upgrade until the next auto-upgrade cycle.

How to upgrade an excluded client

If a device is a member of a collection that you excluded from upgrade, you can still upgrade the client using one of the following methods:

- **Client push installation**: Ccmsetup allows client push installation because it's your direct intent. This method lets you upgrade a client without removing it from the collection, or removing the entire collection from exclusion.
- **Manual client installation**: Manually upgrade an excluded client by using the following Ccmsetup command-line parameter: **/IgnoreSkipUpgrade**

  If you attempt to manually upgrade a client that's a member of the excluded collection, and don't use this

parameter, the client doesn't upgrade. For more information, see How to install Configuration Manager clients manually.

See also

- Upgrade clients
- How to deploy clients to Windows computers
- Extended interoperability client

How to upgrade clients for Windows computers in Configuration Manager

9/11/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Upgrade the Configuration Manager client on Windows computers using client installation methods or the automatic client upgrade feature. The following client installation methods are valid ways to upgrade client software on Windows computers:

- Group policy installation
- Logon script installation
- Manual installation
- Upgrade installation

For more information, see How to deploy clients to Windows computers.

Exclude clients from upgrade by specifying an exclusion collection. For more information, see How to exclude clients from upgrade. Excluded clients still download and run CCMSETUP, but won't upgrade.

> **TIP**
> If upgrade your server infrastructure from a previous version of Configuration Manager, complete the server upgrades before upgrading the Configuration Manager clients. This process includes installing all current branch updates. The latest current branch update contains the latest version of the client. Upgrade clients after you have installed all of the Configuration Manager updates.

> **NOTE**
> If you plan to reassign the site for the clients during upgrade, specify the new site using the `SMSSITECODE` client.msi property. If you use the value of `AUTO` for the `SMSSITECODE`, also specify `SITEREASSIGN=TRUE`. This property allows for automatic site reassignment during upgrade. For more information, see Client installation properties - SMSSITECODE.

About automatic client upgrade

Configure the site to automatically upgrade clients to the latest Configuration Manager version. When Configuration Manager identifies an assigned client's version is earlier than the hierarchy version, it automatically upgrades the client. This scenario includes upgrading the client to the latest version when it attempts to assign to a Configuration Manager site.

A client can automatically upgrade in the following scenarios:

- The client version is earlier than the version used in the hierarchy.
- The client on the central administration site (CAS) has a language pack installed and the existing client doesn't.
- A client prerequisite in the hierarchy is a different version than the one installed on the client.

- One or more of the client installation files are a different version.

> **NOTE**
> To identify the different versions of the Configuration Manager client in your hierarchy, use the report **Count of Configuration Manager clients by client versions** in the report folder **Site - Client Information**.

Configuration Manager creates an upgrade package by default. It automatically sends the package to all distribution points in the hierarchy. If you make changes to the client package on the CAS, Configuration Manager automatically updates the package, and redistributes it. An example change is when you add a client language pack. If you enable automatic client upgrade, every client automatically installs the new client language package.

> **NOTE**
> Configuration Manager doesn't automatically send the client upgrade package to Configuration Manager cloud-based distribution points.

Enable automatic client upgrade across your hierarchy. This configuration keeps your clients up-to-date with less effort.

If you also manage your Configuration Manager site systems as clients, determine whether to include them as part of the automatic upgrade process. You can exclude all servers, or a specific collection from client upgrade. Some Configuration Manager site roles share the client framework. For example, the management point and pull distribution point. These roles upgrade when you update the site, so the client version on these servers updates at the same time.

Configure automatic client upgrade

Use the following procedure to configure automatic client upgrade at the CAS. This configuration applies to all clients in your hierarchy.

1. In the Configuration Manager console, go to the **Administration** workspace, expand **Site Configuration**, and then select the **Sites** node.
2. On the **Home** tab of the ribbon, in the **Sites** group, select **Hierarchy Settings**.
3. Switch to the **Client Upgrade** tab. Review the version and date of the production client. Make sure it's the version you want to use to upgrade your clients. If it's not the client version you expect, you may need to promote the pre-production client to production. For more information, see How to test client upgrades in a pre-production collection.
4. Select **Upgrade all clients in the hierarchy using the production client**. Select **OK** to confirm.
5. If you don't want client upgrades to apply to servers, select **Do not upgrade servers**.
6. Specify the number of days in which devices must upgrade the client. After the device receives policy, it upgrades the client at a random interval within this number of days. This behavior prevents a large number of clients simultaneously upgrading.

> **NOTE**
>
> A computer must be running to upgrade the client. If a computer isn't running when it's scheduled to receive the upgrade, the upgrade doesn't occur. When the computer turns on, and it receives policy, it schedules the upgrade for a random time within the allowed number of days. If this occurs after the number of days to upgrade has expired, it schedules the upgrade at a random time within 24 hours after the computer was turned on.
>
> Because of this behavior, computers that are routinely shut down may take longer to upgrade than expected if the randomly scheduled upgrade time isn't within the normal working hours.

7. To exclude clients from upgrade, select **Exclude specified clients from upgrade**, and specify the collection to exclude. For more information, see Exclude clients from upgrade.
8. If you want the site to copy the client installation package to distribution points that you've enabled for prestaged content, select the option to **Automatically distribute client installation package to distribution points that are enabled for prestaged content**.
9. Select **OK** to save the settings and close Hierarchy Settings Properties.

Clients receive these settings when they next download policy.

> **NOTE**
>
> Client upgrades honor any Configuration Manager maintenance windows you've configured.

Next steps

For alternative methods to upgrade clients, see How to deploy clients to Windows computers.

Exclude specific clients from automatic upgrade. For more information, see How to exclude clients from upgrade.

How to upgrade clients for Linux and UNIX servers in Configuration Manager

3/27/2019 • 4 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

> **IMPORTANT**
>
> Starting in version 1902, Configuration Manager doesn't support Linux or UNIX clients.
>
> Consider Microsoft Azure Management for managing Linux servers. Azure solutions have extensive Linux support that in most cases exceed Configuration Manager functionality, including end-to-end patch management for Linux.

You can upgrade the version of the client for Linux and UNIX on a computer to a newer client version without first uninstalling the current client. To do so, install the new client installation package on the computer while using the **-keepdb** command-line property. When the client for Linux and UNIX installs, it overwrites existing client data with the new client files. However, the **-keepdb** command-line property directs the install process to retain the clients unique identifier (GUID), local database of information, and certificate store. This information is then used by the new client installation.

For example, you have a RHEL5 x64 computer that runs the client from the original release of the Configuration Manager client for Linux and UNIX. To upgrade this client to the client version from cumulative update 1, you manually run the **install** script to install the applicable client package from cumulative update 1, with the addition of the **-keepdb** command-line switch. See the following example command line:

```
./install -mp <hostname\> -sitecode <code\> -keepdb ccm-Universal-x64.<build\>.tar
```

How to use a Software Deployment to Upgrade the Client on Linux and UNIX Servers

You can use a software deployment to upgrade the client for Linux and UNIX to a new client version. However, the Configuration Manager client can't directly run the installation script to install the new client because the installation of a new client must first uninstall the current client. This action would end the Configuration Manager client process that runs the installation script before the installation of the new client begins. To successfully use a software deployment to install the new client, you must schedule the installation to start at a future time and to be run by the operating system's built-in scheduling capabilities.

Use a software deployment to first copy the files for the new client installation package to the client computer. Then deploy and run a script to schedule the client installation process. The script uses the operating system's built-in **at** command to delay its start. When the script runs, its operation is managed by the client operating system and not the Configuration Manager client on the computer. This behavior allows the command line called by the script to first uninstall the Configuration Manager client, and then install the new client. These actions complete the process of client upgrade on the Linux or UNIX computer. After the upgrade completes, the upgraded client remains managed by Configuration Manager.

Use the following procedure to help you configure a software deployment to upgrade the client for Linux and UNIX. The following steps and examples upgrade a RHEL5 x64 computer that runs the initial release of the client to the cumulative update 1 client version.

To use a software deployment to upgrade the client on Linux and UNIX servers

1. Copy the new client installation package to the computer that runs the Configuration Manager client to upgrade.

   For example, place the client installation package and install script for cumulative update 1 in the following location on the client computer: **/tmp/PATCH**

2. Create a script to manage the upgrade of the Configuration Manager client. Then place a copy of the script in the same folder on the client computer as the client installation files from step 1.

   The script doesn't require a specific name. It must contain command lines sufficient to use the client installation files from a local folder on the client computer, and to install the client installation package by using the **-keepdb** command-line property. Use the **-keepdb** command-line property to maintain the unique identifier of the current client for use by the new client you're installing.

   For example, create a script named **upgrade.sh** that contains the following lines:

   ```
   #!/bin/sh
   #
   /tmp/PATCH/install -sitecode <code> -mp <hostname> -keepdb /tmp/PATCH/ccm-Universal-x64.<build>.tar
   ```

   Then copy it to the **/tmp/PATCH** folder on the client computer.

3. Use software deployment to have each client use the computers built-in **at** command to run the **upgrade.sh** script with a short delay before the script runs.

   For example, use the following command line to run the script: **at -f /tmp/upgrade.sh -m now + 5 minutes**

   After the client successfully schedules the **upgrade.sh** script to run, the client submits a status message indicating the software deployment completed successfully. However, the actual client installation is then managed by the computer, after the delay. After the client upgrade completes, validate the install by reviewing the **/var/opt/microsoft/scxcm.log** file on the client computer. Confirm the client is installed and communicating with the site by viewing details for the client in the **Devices** node of the **Assets and Compliance** workspace in the Configuration Manager console.

How to upgrade clients on Mac computers in Configuration Manager

9/11/2019 • 2 minutes to read • Edit Online

Applies to: System Center Configuration Manager (Current Branch)

Follow the high-level steps in this article to upgrade the client for Mac computers by using a Configuration Manager application. You can also download the Mac client installation file, copy it to a shared network location or a local folder on the Mac computer, and then instruct users to manually run the installation.

> **NOTE**
> Before you do these steps, make sure that your Mac computer meets the prerequisites. See Supported operating systems for Mac computers.

Download the latest Mac client

The Mac client for Configuration Manager isn't supplied on the Configuration Manager installation media. Download it from the Microsoft Download Center. The Mac client installation files are contained in a Windows Installer file named **ConfigmgrMacClient.msi**.

Create the Mac client installation file

On a computer that runs Windows, run **ConfigmgrMacClient.msi**. This installer unpacks the Mac client installation file, named **Macclient.dmg**. By default, you can find this file in the following folder: **C:\Program Files (x86)\Microsoft\System Center 2012 Configuration Manager Mac Client**.

Extract the client installation files

Copy **Macclient.dmg** to a Mac computer. Mount the Macclient.dmg file in macOS, and then copy the contents to a folder on the Mac computer.

Create a .cmmac file

1. Open the **Tools** folder of the Mac client installation files. Use the **CMAppUtil** tool to create a .cmmac file from the client installation package. You'll use this file to create the Configuration Manager application.
2. Copy the new **CMClient.pkg.cmmac** file to a network location that's available to the computer running the Configuration Manager console.

   For more information, see the Supplemental procedures to create and deploy applications for Mac computers.

Create and deploy the app

1. In the Configuration Manager console, create an application from the **CMClient.pkg.cmmac** file.
2. Deploy this application to Mac computers in your hierarchy.

Install the updated client

The existing Configuration Manager client on Mac computers will prompt the user that an update is available to install. After users install the client, they must restart their Mac computer.

After the computer restarts, the **Computer Enrollment** wizard automatically runs to request a new user certificate.

If you don't use Configuration Manager enrollment, but install the client certificate independently from Configuration Manager, see Configure clients to use an existing certificate.

Configure clients to use an existing certificate

Use this procedure to prevent the Computer Enrollment Wizard from running, and to configure the upgraded client to use an existing client certificate.

1. In the Configuration Manager console, create a configuration item of the type **Mac OS X**.
2. Add a setting to this configuration item with the setting type **Script**.
3. Add the following script to the setting:

```
#!/bin/sh
echo "Starting script\n"
echo "Changing directory to MAC Client\n"
cd /Users/Administrator/Desktop/'MAC Client'/
echo "Import root cert\n"
/usr/bin/sudo /usr/bin/security import /Users/Administrator/Desktop/'MAC Client'/Root.pfx -A -k
/Library/Keychains/System.Keychain -P ROOT
echo "Using openssl to convert pfx to a crt\n"
/usr/bin/sudo openssl pkcs12 -in /Users/Administrator/Desktop/'MAC Client'/Root.pfx -out Root1.crt -nokeys -
clcerts -passin pass:ROOT
echo "Adding trust to root cert\n"
/usr/bin/sudo /usr/bin/security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.Keychain
Root1.crt
echo "Import client cert\n"
/usr/bin/sudo /usr/bin/security import /Users/Administrator/Desktop/'MAC Client'/MacClient.pfx -A -k
/Library/Keychains/System.Keychain -P MAC
echo "Executing ccmclient with MP\n"
sudo ./ccmsetup -MP https://SCCM34387.SCCM34387DOM.NET/omadm/cimhandler.ashx
echo "Editing Plist file\n"
sudo /usr/libexec/Plistbuddy -c 'Add:SubjectName string CMMAC003L' /Library/'Application
Support'/Microsoft/CCM/ccmclient.plist
echo "Changing directory to CCM\n"
cd /Library/'Application Support'/Microsoft/CCM/
echo "Making connection to the server\n"
sudo open ./CCMClient
echo "Ending Script\n"
exit
```

1. Add the configuration item to a configuration baseline. Then deploy the configuration baseline to all Mac computers that install a certificate independently from Configuration Manager.