**Test Lab Guide: Deploying an AD CS Two-Tier PKI Hierarchy**

Published: February 8, 2012

Updated: August 9, 2012

Applies To: Windows Server 2012

The purpose of this Test Lab Guide (TLG) is to enable you to create a two-tier public key infrastructure (PKI) hierarchy using Windows Server® 2012 and Active Directory Certificate Services (AD CS).

[In this guide](javascript:void(0))

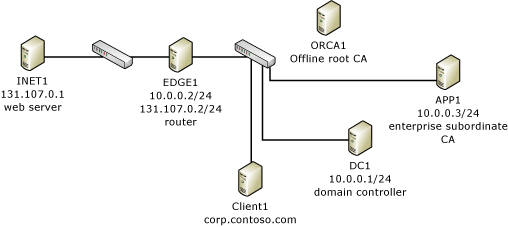
This document contains instructions for extending the Windows Server 2012 Base Configuration Test Lab Guide (TLG) to include an offline root certification authority and install an online enterprise subordinate certification authority on the computer APP1 from the Base Configuration TLG. In this guide you will deploy a two-tier PKI hierarchy, configure a certificate revocation list (CRL) distribution point (CDP), automatically deploy certificates to the domain, and utilize a certificate to enable Secure Sockets Layer (SSL) communication with the APP1 web site.

|  |
| --- |
| **ImportantImportant** |
| The configuration of the computers and network in this guide was designed to give you hands-on practice in creating a two-tier certification authority PKI hierarchy. The design decisions made in this guide were geared toward increasing your hands-on experience and do not reflect a best practices configuration. For best practice information, see [Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure](http://technet.microsoft.com/library/cc772670.aspx) (http://technet.microsoft.com/library/cc772670.aspx) and [PKI Design Brief Overview](http://social.technet.microsoft.com/wiki/contents/articles/pki-design-brief-overview.aspx) (http://social.technet.microsoft.com/wiki/contents/articles/pki-design-brief-overview.aspx). |

[Test lab overview](javascript:void(0))

The test lab configuration demonstrated in this guide extends the Windows Server 2012 Base Configuration TLG by one server computer. The additional computer will serve as an offline root CA and be named ORCA1. There are six major steps in this test lab guide to complete that include multiple subordinate procedures.

1. Complete the Base TLG Configuration
2. Configure ORCA1
3. Configure APP1 to distribute certificates and CRLs
4. Configure APP1 as an enterprise subordinate CA
5. Enable certificate auto-enrollment
6. Configure SSL for APP1



[Hardware and software requirements](javascript:void(0))

The following are the minimum required components of the test lab:

1. The product disc or files for Windows Server 2012.
2. The product disc or files for Windows Server 2012.
3. Five computers that meet the minimum hardware requirements for Windows Server 2012. One of these computers (EDGE1) has two network adapters installed.
4. One computer that meets the minimum hardware requirements for Windows® 8.

|  |
| --- |
| **noteNote** |
| You will need only the DC1, APP1, and CLIENT1 computers from the Base Test Lab configuration to complete this lab. You will also build the ORCA1 computer during this lab. |

1. One removable media with enough free space to hold a few certificates and certificate revocation lists (about 10 kilobytes). This can be either physical or virtual removable media depending on whether your lab is using physical or virtual computers.

|  |
| --- |
| **noteNote** |
| For instructions on transferring files using a virtual floppy disk using Microsoft Windows Server™ Hyper-V, see [Creating, Using, and Transferring Files using Virtual Floppy Disks](http://social.technet.microsoft.com/wiki/contents/articles/4272.aspx) (http://social.technet.microsoft.com/wiki/contents/articles/4272.aspx). |

1. If you wish to deploy the Base Configuration test lab in a virtualized environment, your virtualization solution must support Windows Server 2012 64-bit virtual machines. The server hardware must support the amount of RAM required to run the virtual operating systems included in the Base Configuration test lab and any other virtual machines that may be required by additional TLGs.

|  |
| --- |
| **ImportantImportant** |
| Run Windows Update on all computers or virtual machines either during the installation or immediately after installing the operating systems. After running Windows Update, you can isolate your physical or virtual test lab from your production network. |

[Step 1: Complete the Base TLG Configuration](javascript:void(0))

The Windows Server 2012 Base Configuration Test Lab Guide (TLG) is located at <http://go.microsoft.com/fwlink/p/?LinkId=236358>.

[Step 2: Configure ORCA1](javascript:void(0))

The procedures to complete the configuration of the offline root CA, named ORCA1, include:

* Install the Operating system
* Rename the computer
* Prepare the CAPolicy.inf for the standalone root CA
* Install the standalone root CA
* Configure the root CA settings
* Copy the root CA certificate and CRL to removable media
* Distribute the root CA via GPO
* Create an internal contoso.com DNS zone and www host record

[To install the operating system on ORCA1](javascript:void(0))

1. Do not connect this computer to a network.
2. Start the installation of Windows Server 2012.
3. Follow the instructions to complete the installation, specifying Windows Server 2012 (full installation) and a strong password for the local Administrator account. Sign in using the local Administrator account.

[To rename the computer](javascript:void(0))

1. Open Windows PowerShell®.
2. Type **rename-computer orca1** and then press ENTER.
3. Type **restart-computer** and then press ENTER.

After the computer restarts, sign in using the local Administrator account.

[To prepare the CAPolicy.inf for the standalone root CA](javascript:void(0))

1. Open Windows PowerShell, type **notepad c:\Windows\CAPolicy.inf** and press ENTER.
2. When prompted to create a new file, click **Yes**.
3. Enter the following as the contents of the file:

[Copy](javascript:CodeSnippet_CopyCode('CodeSnippetContainerCode_5b046f8e-14af-4412-b1c2-3133de8cf13a');" \o "Copy to clipboard.)

[Version]

Signature="$Windows NT$"

[PolicyStatementExtension]

Policies=InternalPolicy

[InternalPolicy]

OID= 1.2.3.4.1455.67.89.5

Notice="Legal Policy Statement"

URL=http://www.contoso.com/pki/cps.txt

[Certsrv\_Server]

RenewalKeyLength=2048

RenewalValidityPeriod=Years

RenewalValidityPeriodUnits=20

CRLPeriod=weeks

CRLPeriodUnits=26

CRLDeltaPeriod=Days

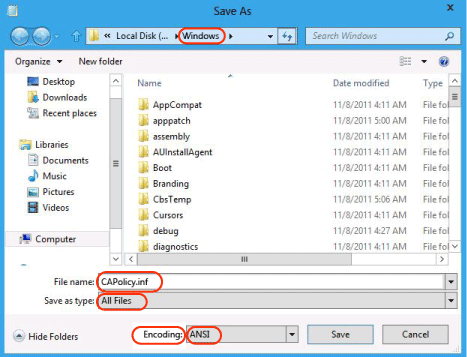
CRLDeltaPeriodUnits=0

LoadDefaultTemplates=0

AlternateSignatureAlgorithm=1

|  |
| --- |
| **noteNote** |
| The OID shown in the example is the Microsoft OID. Individual organizations should obtain their own OIDs. For more information about OIDs, see Obtaining a Root OID from an ISO Name Registration Authority (http://msdn.microsoft.com/library/windows/desktop/ms677621.aspx). |
| **TipTip** |
| Setting the CRLDeltaPeriodUnits=0 in the CAPolicy.inf disables Delta CRL publishing, which is the appropriate setting for an offline Root CA. |

1. Click **Save As**. Ensure the following:
   * **File name** is set to **CAPolicy.inf**
   * **Save as type** is set to **All Files**
   * **Encoding** is **ANSI**
2. When you are prompted to overwrite the file, click **Yes**.



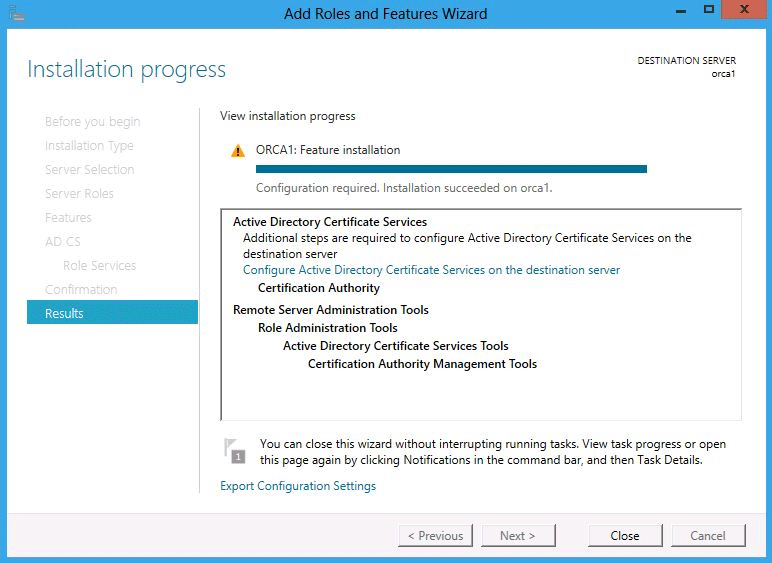
|  |
| --- |
| **CautionCaution** |
| Be sure to save the CAPolicy.inf with the inf extension. If you do not specifically type **.inf** at the end of the file name and select the options as described, the file will be saved as a text file and will not be used during CA installation. |

1. Close Notepad.

|  |
| --- |
| **ImportantImportant** |
| In the CAPolicy.inf, you can see there is a line specifying the URL http://www.contoso.com/pki/cps.txt. The Internal Policy section of the CAPolicy.inf is just shown as an example of how you would specify the location of a certificate practice statement (CPS). To learn more about policy statements including CPS, see [Creating Certificate Policies and Certificate Practice Statements](http://technet.microsoft.com/library/cc780454.aspx) (http://technet.microsoft.com/library/cc780454.aspx) and [RFC 2527](http://www.ietf.org/rfc/rfc2527.txt) (http://www.ietf.org/rfc/rfc2527.txt). For more information about CAPolicy.inf file syntax and purposes, see [CA Policy.inf Syntax](http://technet.microsoft.com/library/cc728279.aspx) (http://technet.microsoft.com/library/cc728279.aspx). |

[To install the standalone root CA](javascript:void(0))

1. In Server Manager, click **Manage**, and then click **Add Roles and Features**.
2. On the **Before you begin** screen, click **Next**.
3. On the **Select installation type** screen, ensure the default selection of **Role-based or feature-based installation** is selected. Click **Next**.
4. On the **Select destination server** screen, ensure that **orca1** is selected and then click **Next**.
5. On the **Select server roles** screen, select the **Active Directory Certificate Services** role.
6. When prompted to install **Remote Server Administration Tools** click **Add Features**. Click **Next**.
7. On the **Select features** screen, click **Next**.
8. On the **Active Directory Certificate Services** screen, click **Next**.
9. On the **Select role services** screen, the **Certification Authority** role is selected by default. Click **Next**.
10. On the **Confirm installation selections** screen, verify the information and then click **Install**.
11. Wait for the installation to complete. The installation progress screen is displayed while the binary files for the CA are installed. When the binary file installation is complete, click the **Configure Active Directory Certificate Services on the destination server** link.



|  |
| --- |
| **TipTip** |
| If you were to click **Close** before the installation completed, you could complete the configuration of the role service by through a link to complete the configuration in the notifications icon of Server Manager. |

1. On the **Credentials** screen, you should see that the **ORCA1\Administrator** is displayed in the **Credentials** box. Click **Next**.

|  |
| --- |
| **noteNote** |
| When installing a Standalone CA, you must use an account that is a member of the local **Administrators** group. |

1. On the **Role Services** screen, select **Certification Authority**. This is the only available selection when only the binary files for the certification authority role are installed on the server. Click **Next**.
2. The only selection available on the **Setup Type** screen is **Standalone CA**. This is because the account used to install is a member of the local Administrators group and the server is not a member of an Active Directory Domain Services (AD DS) domain. Click **Next**.
3. On the **CA Type** screen, **Root CA** is selected by default. Click **Next**.
4. On the **Private Key** screen, leave the default selection to **Create a new private key** selected. Click **Next**.
5. On the **Cryptography for CA** screen, ensure that the cryptographic provider is **RSA#Microsoft Software Key Storage Provider**, the key length is set to **2048** and the hash algorithm is set to **SHA1** then click **Next**.

|  |
| --- |
| **noteNote** |
| Do not select the **Allow administrator interaction when the private key is accessed by the CA** checkbox. This setting is typically used with Hardware Security Modules (HSMs) and similar key protection devices prompt for additional information when the private key is accessed. |

1. On the **CA Name** screen, in the **Common name for this CA** text box, type **ContosoRootCA** and then click **Next**.
2. On the **Validity Period** screen, enter **20** for the number of years for the certificate to be valid.
3. On the **CA Database** screen, leave the default locations for the database and database log files. Click **Next**.
4. On the **Confirmation** screen, click **Configure**.
5. The **Progress** screen is displayed during the configuration processing, then the **Results** screen appears. Click **Close**. If the **Installation progress** screen is still open, click **Close** on that screen as well.

|  |
| --- |
| **TipTip** |
| The following Windows PowerShell commands would perform the same action as shown above  Add-WindowsFeature Adcs-Cert-Authority -IncludeManagementTools  Install-AdcsCertificationAuthority –CAType StandaloneRootCA –CACommonName “ContosoRootCA” –KeyLength 2048 –HashAlgorithm SHA1 –CryptoProviderName “RSA#Microsoft Software Key Storage Provider” |

[To configure the root CA settings](javascript:void(0))

1. In Server Manager, click **Tools** and then click **Certification Authority**.
2. In the Certification Authority console tree, expand **ORCA1-CA**. Right-click **Revoked Certificates** and then click **Properties**.
3. On the **CRL Publishing Parameters** tab, ensure that **Publish Delta CRLs** is cleared (not selected). Click **OK**.
4. In the Certification Authority console tree, right-click **ORCA1-CA** and then click **Properties**.
5. Click the **Extensions** tab. Ensure that **Select extensions** is set to **CRL Distribution Point (CDP)** and in the **Specify locations from which users can obtain a certificate revocation list (CRL)**, review the default settings.
6. Change **Select extension** to **Authority Information Access (AIA)** and review the default settings. Click **OK**. If you are prompted to restart Active Directory Certificate Services, click **No**. You will restart the service after modifying the default paths in the next step.
7. From Windows PowerShell run the following commands:   
   certutil -setreg CA\CRLPublicationURLs "1:C:\Windows\system32\CertSrv\CertEnroll\%3%8.crl\n2:http://www.contoso.com/pki/%3%8.crl"  
     
   certutil –setreg CA\CACertPublicationURLs "2:http://www.contoso.com/pki/%1\_%3%4.crt"  
     
   restart–service certsvc  
     
   certutil -crl

|  |
| --- |
| **noteNote** |
| The two certutil commands above set the CDP and AIA paths respectively for the Root CA. The same configuration can be accomplished using the following PowerShell cmdlet commands:  $crllist = Get-CACrlDistributionPoint; foreach ($crl in $crllist) {Remove-CACrlDistributionPoint $crl.uri -Force};  Add-CACRLDistributionPoint -Uri C:\Windows\System32\CertSrv\CertEnroll\%3%8.crl -PublishToServer -Force  Add-CACRLDistributionPoint -Uri http://www.contoso.com/pki/%3%8.crl -AddToCertificateCDP -Force  $aialist = Get-CAAuthorityInformationAccess; foreach ($aia in $aialist) {Remove-CAAuthorityInformationAccess $aia.uri -Force};  Add-CAAuthorityInformationAccess -AddToCertificateAia http://www.contoso.com/pki/%1\_%3%4.crt -Force |

To view the AIA and CDP, you can run the following commands: Get-CAAuthorityInformationAccess | format-list and Get-CACRLDistributionPoint | format-list. You can also return to the **Extensions** tab in certification authority properties dialog box and see the changes made to the AIA and CDP.

[To copy the root CA certificate and CRL to removable media](javascript:void(0))

1. From Windows PowerShell, run the command **dir C:\Windows\system32\certsrv\certenroll\\*.cr\***, which displays the certificates and CRLs in the default certificate store.
2. Copy the CA certificate file and CRL to removable media. For example, if you were running commands to copy the certificate and CRL to a floppy disk drive (A:), you would run the following commands:
   1. **copy C:\Windows\system32\certsrv\certenroll\\*.cr\* A:\**
   2. **dir A:\**

|  |
| --- |
| **TipTip** |
| Substitute the drive letter of your removable media for A: in the commands shown above. The removable media can be either physical or virtual, as discussed in [Hardware and software requirements](http://technet.microsoft.com/en-us/library/hh831348.aspx#BKMK_REQ). Also, if you see an error that reads “The volume does not contain a recognized file system.” You may need to format the media. For example, if it is a floppy disk, you might need to type **format a:** and then press ENTER. |

[To distribute the root CA certificate](javascript:void(0))

1. On APP1, sign in using the User1 account, which is a member of both **Domain Admins** and **Enterprise Admins**. Open Windows PowerShell as administrator. To do so, right-click the Windows PowerShell icon and then click **Run as administrator**. When prompted by User Account Control, click **Yes**.
2. Insert the removable media containing the offline root CA certificate into APP1.
3. From Windows PowerShell change to the removable media drive using the cd command (as in run **cd a:\** to change to the root of drive A).
4. From the Windows PowerShell on the removable media drive, run the following commands:   
   certutil –dspublish –f orca1\_ContosoRootCA.crt RootCA  
     
   certutil –addstore –f root orca1\_ContosoRootCA.crt  
     
   certutil –addstore –f root ContosoRootCA.crl

|  |
| --- |
| **noteNote** |
| The first command places the root CA public certificate into the Configuration container of Active Directory. Doing so allows domain client computers to automatically trust the root CA certificate and there is no additional need to distribute that certificate in Group Policy. The second and third commands place the root CA certificate and CRL into the local store of APP1. This provides APP1 immediate trust of root CA public certificate and knowledge of the root CA CRL. APP1 could obtain the certificate from Group Policy and the CRL from the CDP location, but publishing these two items to the local store on APP1 is helpful to speed the configuration of APP1 as a subordinate CA. |

The public certificates, certificate revocation lists, and certificate practices statement are all to be placed in the location http://www.contoso.com/pki. Internal client computers will not be able to resolve this computer name to the internal web site (APP1) unless an appropriate DNS entry is placed on the DNS server.

[To create a contoso.com DNS zone and www host record](javascript:void(0))

1. On DC1, open the DNS console. In Server Manager, click **Tools**, then click **DNS**.
2. In the DNS console, expand the following in the console tree: **DC1**, **Forward Lookup Zones**.
3. Right-click the **Forward Lookup Zones** and then click **New Zone**.
4. On the **Welcome to the New Zone Wizard** screen, click **Next**.
5. By default you will see that **Primary zone** is selected and that the zone will be stored in Active Directory. To accept these defaults, click **Next**.
6. Leave the default setting and then click **Next**.
7. On **Zone name** screen, type **contoso.com** and then click **Next**.
8. On the **Dynamic Update** screen, leave the default setting and then click **Next**.
9. On the **Completing the New Zone Wizard**, click **Finish**.
10. In the console tree of the DNS console, right-click the **contoso.com** zone and then click **New Host (A or AAAA)**.

|  |
| --- |
| **TipTip** |
| You may have to click the corp.contoso.com zone one time before you are able to access the right-click options. |

1. In **Name (uses parent domain if left blank)**, type **www**.
2. In **IP Address**, type **10.0.0.3**. This zone and record will direct communications from internal clients for www.contoso.com to the address of APP1. Click **Add Host**.
3. Click **OK** to confirm that the record was created. Click **Done**.
4. Close the DNS console

[Step 3: Configure APP1 to distribute certificates and CRLs](javascript:void(0))

In the extensions of the root CA, it was stated that the CRL from the root CA would be available via http://www.contoso.com/pki. Currently, there is not a PKI virtual directory on APP1, so one must be created. In a production environment, you would typically separate the issuing CA role from the role of hosting the AIA and CDP. However, this lab combines both in order to reduce the number of resources needed to complete the lab.

|  |
| --- |
| **TipTip** |
| If a CA cannot find the CRLs of its parent CA, the AD DS service (certsvc) will fail to start on the subordinate CA. This can only be remedied by resolving the CRL distribution issue (recommended) or by changing the CA log level from the default of 3 to level 2. For more information on CA log levels, see [Microsoft Knowledge Base article 305018](http://support.microsoft.com/kb/305018) http://support.microsoft.com/kb/305018. |

[To configure APP1 to distribute certificates and CRLs](javascript:void(0))

1. Ensure that you sign in using the User1 account. Run Windows PowerShell as Administrator and then run the following commands:

New-item -path c:\pki –type directory

write-output "Example CPS statement" | out-file c:\pki\cps.txt

new-smbshare -name pki c:\pki -FullAccess SYSTEM,"CORP\Domain Admins" -ChangeAccess "CORP\Cert Publishers"

1. Open the IIS console. In Server Manager, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the Internet Information Services (IIS) Manager console tree, expand **APP1**. If you are invited to get started with Microsoft Web Platform, click **Cancel**.
3. Expand **Sites** and then right-click the **Default Web Site** and then click **Add Virtual Directory**.
4. In **Alias**, type **pki** and then in physical path type **C:\pki**, then click **OK**.
5. Enable Anonymous access to the pki virtual directory. To do so:
   1. In the **Connections** pane, ensure that **pki** is selected.
   2. On **pki Home** click **Authentication**.
   3. In the **Actions** pane, click **Edit Permissions**.
   4. On the **Security** tab, click **Edit**
   5. On the **Permissions for pki** dialog box, click **Add**.
   6. On **Select Users, Computers, Service Accounts, or Groups**, type **Cert Publishers** and then click **Check Names**.
   7. On **Select Users, Computers, Service Accounts, or Groups**, click **Object Types**.
   8. On **Object Types**, select **Service Accounts** and then click **OK**.
   9. On **Select Users, Computers, Service Accounts, or Groups**, click **Locations**.
   10. On **Locations**, click **APP1** and then click **OK**.
   11. On **Select Users, Computers, Service Accounts, or Groups** after **Cert Publishers**, type **;IIS AppPool\DefaultAppPool** and then click **Check Names**. Click **OK**.

|  |
| --- |
| **noteNote** |
| These steps have granted the IIS default application pool **Read & execute**, **List folder contents**, and **Read** permissions. IIS uses the default application pool to allow anonymous access. This will allow users to check the AIA and CDP hosted on IIS. |

* 1. On **Permissions for pki** select **Cert Publishers (CORP\Cert Publishers)**. Under **Permissions for Cert Publishers**, select the **Modify** checkbox in the **Allow** column and then click **OK**. Close the **pki Properties** dialog box.

|  |
| --- |
| **noteNote** |
| Granting modify permissions to the pki folder to **Cert Publishers** allows for the publishing of certificates and CRLs by CAs in the enterprise to the folder. |

1. In the **pki Home** pane, double-click **Request Filtering**.
2. The **File Name Extensions** tab is selected by default in the **Request Filtering** pane. In the **Actions** pane, click **Edit Feature Settings**.
3. In **Edit Request Filtering Settings**, select **Allow double escaping** and then click **OK**. Close Internet Information Services (IIS) Manager.

|  |
| --- |
| **noteNote** |
| Allowing double escaping is needed if you are publishing Delta CRLs to IIS because the Delta CRL file contains a + symbol. For more information, see [Microsoft Knowledge Base article 942076](http://support.microsoft.com/kb/942076) (http://support.microsoft.com/kb/942076). |

1. Run Windows PowerShell as an administrator. From Windows PowerShell, run the command iisreset

[Step 4: Configure APP1 as an Enterprise Subordinate CA](javascript:void(0))

The steps to configure APP1 as an Enterprise Subordinate CA include the following procedures:

1. Configure the CAPolicy.inf
2. Install the enterprise subordinate CA role
3. To configure the AIA and CDP

[To configure the CAPolicy.inf](javascript:void(0))

1. On APP1, as User1, open Windows PowerShell as Administrator and then type **notepad c:\Windows\CAPolicy.inf** and press ENTER.
2. When asked if you want to create the file. Click **Yes**.
3. Use the following information for the enterprise subordinate CA CAPolicy.inf file.

[Copy](javascript:CodeSnippet_CopyCode('CodeSnippetContainerCode_a4d61bae-7cc6-42fc-bce7-dab14024b022');)

[Version]

Signature="$Windows NT$"

[PolicyStatementExtension]

Policies=InternalPolicy

[InternalPolicy]

OID= 1.2.3.4.1455.67.89.5

Notice="Legal Policy Statement"

URL=http://www.contoso.com/pki/cps.txt

[Certsrv\_Server]

RenewalKeyLength=2048

RenewalValidityPeriod=Years

RenewalValidityPeriodUnits=5

LoadDefaultTemplates=0

AlternateSignatureAlgorithm=1

|  |
| --- |
| **CautionCaution** |
| Windows XP clients do not support the Alternate Signature Algorithm. If you want Windows XP clients to be able to enroll for certificates, do not add the line AlternateSignatureAlgorithm=1 to the CAPolicy.inf. For more information, see [Guidelines for Using Alternate Signature Formats](http://technet.microsoft.com/library/cc753169.aspx) (http://technet.microsoft.com/library/cc753169.aspx). |

1. Click **File**, **Save As** and ensure that you are saving an **ANSI** file named **CAPolicy.inf** in the **C:\Windows** folder. You will have to switch the **Save as type** to **All Files** in order to get the inf extension instead of txt extension. When prompted to replace CAPolicy.inf, click **Yes**.
2. Close Notepad.

[To install the enterprise subordinate CA role](javascript:void(0))

1. On APP1, as User1, run Windows PowerShell as Administrator, and then run the following command gpupdate /force. This action ensures that the GPO for the trusted root certification authority is applied to APP1.
2. In Server Manager, click **Manage**, and then click **Add Roles and Features**.
3. On the **Before you begin**, click **Next**.
4. On the **Select installation type** screen, ensure the default selection of **Role or Feature Based Install** is selected. Click **Next**.
5. On the **Select destination server** screen, ensure that **APP1** is selected and then click **Next**.
6. On the **Select server roles** screen, select the **Active Directory Certificate Services** role.
7. When prompted to install **Remote Server Administration Tools** click **Add Features**. Click **Next**.
8. On the **Select features** screen, click **Next**.
9. On the **Active Directory Certificate Services** screen, click **Next**.
10. On the **Select role services** screen, ensure **Certification Authority** is selected and then click **Next**.
11. On the **Confirm installation selections** screen, verify the information and then click **Install**.
12. Wait for the installation to complete. The installation progress screen is displayed while the binary files for the CA are installed. When the binary file installation is complete, click the **Configure Active Directory Certificate Services on the destination server** link.

|  |
| --- |
| **TipTip** |
| If you clicked **Close** before the installation completed, you could complete the configuration of the role service by through a link to complete the configuration in the notifications icon of Server Manager. |

1. On the **Credentials** screen, the credentials for User1 appear. Click **Next**.
2. On the **Role Services** screen, select **Certification Authority**.
3. On the **Setup Type** screen, ensure that **Enterprise CA** is selected and then click **Next**.

|  |
| --- |
| **noteNote** |
| If the computer is a domain member and the credentials supplied previously were for an account that is a member of the **Enterprise Admins** group, you can select **Enterprise CA** or **Standalone CA**. If the computer is not a domain member or credentials were entered for an account that is not a member of **Enterprise Admins**, then only the **Standalone CA** selection is available. |

1. On the **CA Type** screen, select **Subordinate CA** to install an Enterprise Subordinate CA. Click **Next**.
2. On the **Private Key** screen, ensure the **Create a new private key** option is selected and then click **Next**.
3. The **Cryptography for CA** screen, ensure that the cryptographic provider is **RSA#Microsoft Software Key Storage Provider**, key length is **2048**, and the hash algorithm is set to **SHA1**. Click **Next**.
4. On the **CA Name** screen, in **Common name for this CA**, type **IssuingCA-APP1**. You will see that the distinguished name changes to **CN=IssuingCA-APP1,DC=corp,DC=contoso,DC=com**. Click **Next**.
5. On the **Certificate Request** screen, notice that **Save a certificate request to file on the target machine** is selected. This is the correct option because we are using an offline parent CA (the root CA) in this configuration. Leave the default and click **Next**.
6. On the **CA Database** screen, leave the default database and log locations and then click **Next**.
7. On the **Confirmation** screen, click **Configure**.
8. On the **Results** screen, you see that you must take the certificate request to the ContosoRootCA in order to complete the configuration. Click **Close**

|  |
| --- |
| **noteNote** |
| The Windows PowerShell commands to perform the installation of the Enterprise Subordinate CA as shown in this section are:  Add-WindowsFeature Adcs-Cert-Authority -IncludeManagementTools  Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCA -CACommonName "IssuingCA-APP1" -KeyLength 2048 -HashAlgorithm SHA1 -CryptoProviderName "RSA#Microsoft Software Key Storage Provider" |

1. Copy the certificate request to removable media to take to the ORCA1. For example, if you wanted to copy the file from the C:\ drive to a floppy drive with drive letter A:\, then you could run the following command from Windows PowerShell: **copy C:\\*.req A:\**
2. Take the removable media with the certificate request file to the ORCA1. Sign on to the root CA using an account that is a member of local **Administrators**.
3. On ORCA1, from Windows PowerShell, submit the request using the following command (assuming that A:\ is your removable media drive letter):   
   **certreq -submit A:\APP1.corp.contoso.com\_IssuingCA-APP1.req**

|  |
| --- |
| **noteNote** |
| If the removable media has a different drive letter, then substitute that letter for A:\. |

1. On **Certification Authority List**, ensure that **ContosoRootCA (Kerberos)** CA is selected and then click **OK**. You see that the certificate request is pending and the request identification number. Ensure that you note the request ID number.
2. On ORCA1, in Server Manager, click **Tools**, and then click **Certification Authority**. Expand the **ContosoRootCA** object and then click **Pending Requests**.
3. Right-click the Request ID that corresponds with the one you saw when you submitted the request in the previous step. Click **All Tasks** and then click **Issue**.
4. Click **Issued Certificates** and see the issued certificate in the **Details** pane.
5. On ORCA1, return to the command prompt and retrieve the issued certificate by running the command   
   **certreq –retrieve** *<RequestId>* *<drive>***:\APP1.corp.contoso.com\_corp-APP1-CA.crt**.   
   Substitute the actual number of the request when it was submitted for <RequestId> and the actual drive letter of the removable media for <drive>. For example, if the request ID where 2 and the removable media was drive A, then the request would be: certreq –retrieve 2 a:\APP1.corp.contoso.com\_IssuingCA-APP1.crt. When prompted to select the CA, ensure that ORCA1-CA is selected and then click **OK**.
6. On ORCA1, run the command **dir A:\** (assuming that A is the removable media drive letter, if not substitute the correct drive letter for A). You see that ORCA1-CA.crl, orca1\_ORCA1-CA.crt, and APP1.corp.contoso.com\_corp-APP1-CA.crt are now saved to the removable media. Move the removable media to APP1.
7. On APP1, in Windows PowerShell, run the following commands to copy the Certificates and CRLs to the pki folder (assuming that A: is the removable media drive, if not substitute the correct drive letter):   
   copy a:\\*.cr\* c:\pki\
8. On APP1, in the Certification Authority console, right-click the **IssuingCA-APP1**, click **All Tasks**, and then click **Install CA Certificate**.
9. In the **Select file to complete CA installation**, set the file type to **X.509 Certificate (\*.cer; \*.crt)** and then navigate to the removable media and select **APP1.corp.contoso.com\_IssuingCA-APP1.crt**. Click **Open**.
10. Start Active Directory Certificate Services. To do so, right-click **corp-APP1-CA**, click **All Tasks**, and then select **Start Service**.
11. On APP1, copy the CRL from APP1 to the C:\pki folder. From Windows PowerShell, run the command **copy c:\Windows\system32\certsrv\certenroll\\*.cr\* c:\pki\**

|  |
| --- |
| **TipTip** |
| ORCA1 is no longer needed for this lab, so you can turn it off. To turn off a computer from Windows PowerShell, you can run the command stop-computer. |

[To configure the AIA and CDP](javascript:void(0))

1. On APP1, as User1, right-click Windows PowerShell, click **Run as Administrator**. Click **Yes** to confirm that you want to run Windows PowerShell as an Administrator.
2. In Windows PowerShell, run the following commands:   
   certutil -setreg CA\CRLPublicationURLs "65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl\n6:http://www.contoso.com/pki/%3%8%9.crl\n65:file://\\App1.corp.contoso.com\pki\%3%8%9.crl"  
     
   certutil –setreg CA\CACertPublicationURLs "2:http://www.contoso.com/pki/%1\_%3%4.crt\n1:file://\\App1.corp.contoso.com\pki\%1\_%3%4.crt"
3. From Windows PowerShell run the following commands to restart the CA service: restart-service certsvc

|  |
| --- |
| **noteNote** |
| The two certutil commands set the CDP and AIA paths respectively for the CA. The same configuration can be accomplished using the following PowerShell commands:  $crllist = Get-CACrlDistributionPoint; foreach ($crl in $crllist) {Remove-CACrlDistributionPoint $crl.uri -Force};  Add-CACRLDistributionPoint -Uri C:\Windows\System32\CertSrv\CertEnroll\%3%8%9.crl -PublishToServer -PublishDeltaToServer -Force  Add-CACRLDistributionPoint -Uri http://www.contoso.com/pki/%3%8%9.crl -AddToCertificateCDP -Force  Add-CACRLDistributionPoint -Uri file://\\App1.corp.contoso.com\pki\%3%8%9.crl -PublishToServer -PublishDeltaToServer -Force  $aialist = Get-CAAuthorityInformationAccess; foreach ($aia in $aialist) {Remove-CAAuthorityInformationAccess $aia.uri -Force};  Add-CAAuthorityInformationAccess -AddToCertificateAia http://www.contoso.com/pki/%1\_%3%4.crt -Force  Add-CAAuthorityInformationAccess -AddToCertificateAia file://\\App1.corp.contoso.com\pki\%1\_%3%4.crt -Force  By sharing the pki folder and including the file path file://\\App1.corp.contoso.com\pki\%3%8%9.crl as a CDP extension, the CRLs and Delta CRLs will be copied to the share when you run the command certutil –crl. If you want to further restrict access to the share, you could create a separate group and include only the CAs that you want to authorize to publish to the share in that group. Then, share the pki folder only to that specific group and the SYSTEM account. |

1. From Windows PowerShell run the following command to publish the CRL: certutil -crl

|  |
| --- |
| **ImportantImportant** |
| A configuration item that is typically performed on production CAs that is not part of this lab is to enable [Audit Object Access](http://technet.microsoft.com/library/cc776774.aspx) (http://technet.microsoft.com/library/cc776774.aspx) and then to enable all auditing events by running the following command: **certutil -setreg CA\AuditFilter 127**. After doing so, ensure that you regularly archive the Security Event Log and follow the [Auditing Security Events Best Practices](http://technet.microsoft.com/library/cc778162.aspx) (http://technet.microsoft.com/library/cc778162.aspx). |

[Step 5: Configure computer certificate autoenrollment](javascript:void(0))

There are two procedures in order to configure computer certificate autoenrollment:

1. Enable certificate autoenrollment through Group Policy
2. Configure a client and server authentication certificate template for autoenrollment

[To enable certificate autoenrollment through Group Policy](javascript:void(0))

1. On DC1, sign in as User1. In Server Manager, click **Tools**, and then click **Group Policy Management**.
2. On the console tree, expand the following objects: **Forest: corp.contoso.com**, **Domains**, **corp.contoso.com**.

|  |
| --- |
| **noteNote** |
| You might see a warning that any policies linked to the domain will affect all computers to which the policy is linked. If so, read it and then click **OK**. |

1. In the console tree, right-click **Default Domain Policy**, and then click **Edit**.
2. In the console tree of the Group Policy Management Editor, under **Computer Configuration**, expand the following objects: **Policies**, **Windows Settings**, **Security Settings**, and then click **Public Key Policies**.
3. In the details pane, double-click **Certificate Services Client - Auto-Enrollment**. In **Configuration Model**, select **Enabled**.
4. Select **Renew expired certificates, update pending certificates, and remove revoked certificates** and **Update certificates that use certificate templates**. Click **OK**.
5. Close Group Policy Management Editor and Group Policy Management Console.

[To configure a client server authentication certificate template for autoenrollment](javascript:void(0))

1. On APP1, in the Certification Authority console pane, ensure that **IssuingCA-APP1** is expanded.
2. Right-click **Certificate Templates** and then click **Manage**.
3. In the details pane, right-click **Workstation Authentication** and then click **Duplicate Template**.
4. Click the **General** tab, in **Template display name**, type **Client-Server Authentication** and then select **Publish** certificate in Active Directory.
5. Click the **Extensions** tab, ensure **Application Policies** is selected, and then click **Edit**.
6. Click **Add** then click **Server Authentication**. Click **OK** twice.
7. On the **Properties of New Template** dialog, click the **Security** tab.
8. In **Group or user names**, click **Domain Computers (CORP\Domain Computers)**.
9. In the **Autoenroll** row, select the **Allow** checkbox. This will cause all domain computers to automatically enroll for certificates using this template.

|  |
| --- |
| **noteNote** |
| The computers also need Read permission for the template in order to enroll. However, this permission is already granted to the Authenticated Users group. All computer accounts in t domain are members of Authenticated Users, so they already have the permission to Read the template. |

1. Click **OK**. Close the **Certificate Templates Console**.
2. Right-click **Certificate Templates**, click **New**, click **Certificate Template to Issue**.
3. In the **Enable Certificate Templates** dialog box, click **Client-Server Authentication** and then click **OK**. Close the Certification Authority console.

[Step 6: Configuring SSL for APP1](javascript:void(0))

To demonstrate how the certificates deployed through AD DS and AD CS can be used, you will secure the APP1 Web site using SSL and then connect to that secure site with CLIENT1. There are two procedures in this step:

1. Secure the APP1 Default Web Site
2. Connect to the secure web site

[To secure the APP1 Default Web Site](javascript:void(0))

1. On APP1, as User1, run Windows PowerShell as Administrator. Then, run the following commands:

Gpupdate /force. Wait for the update of Group Policy to complete and then close the Command Prompt. This ensures that the autoenrollment certificate distributed through Group Policy is issued to APP1.

cd cert:\LocalMachine\My

dir | format-list

You should see that you have two certificates. One was issued by ContosoRootCA, which is the APP1 CA certificate. The other certificate was issued by IssuingCA-APP1 and it can be used to secure the APP1 default web site.

1. Open the Internet Information Services (IIS) Manager console. To do so, in Server Manager, click **Tools** and then click **Internet Information Services (IIS) Manager**. In the contents pane, expand the following path **APP1**, **Sites**, and **Default Web Site**.

|  |
| --- |
| **noteNote** |
| If you see an Internet Information Services (IIS) Manager prompt asking if you want to get started with Microsoft Web Platform, click **Cancel**. |

1. Click **Default Web Site**. In the **Actions** pane click **Bindings**.
2. In the **Site Bindings** dialog box, click **Add**.
3. In the **Add Site Binding** dialog box, in Type, select **https**.
4. Under **SSL certificate**, click **Select**.
5. In **Select Certificate** use the selection box to select the certificate that was issued by the IssuingCA-APP1 through the Group Policy. This will be a certificate with a long alphanumeric, as opposed one that reads IssuingCA-APP1. To verify you have the correct certificate, click **View**. Ensure the certificate you select shows that it was issued to **APP1.corp.contoso.com** and issued by **IssuingCA-APP1**. Once you have the correct certificate, click **OK** on the **Certificate** dialog box.
6. On **Add Site Binding** dialog box, click **OK**.
7. In the **Site Bindings** dialog box, click **Close**.

[To connect to the secure web site](javascript:void(0))

1. Connect CLIENT1 to the Corporate network.
2. Log on to CLIENT1 as User1.
3. Open Internet Explorer on CLIENT1.
4. In Internet Explorer, enter the address **https://app1.corp.contoso.com** and press ENTER. When you see the default IIS 8 web page, you are confirming that https and the SSL binding are working for the Default Web Site on APP1.

|  |
| --- |
| **TipTip** |
| If instead you see that there is a problem with the certificate, then you probably selected an incorrect certificate in the previous procedure. You must select the certificate that was issued for the name APP1.corp.contoso.com. Also, it could be that Group Policy has not yet updated the Trusted Root Certification authorities. To ensure that the Group Policy updates are in place, open Explorer, then type **cmd** in the Explorer address bar. Then type **gpupdate /force** and press ENTER. |
| **ImportantImportant** | |
| The ORCA1 certificate revocation list (CRL) is valid for 26 weeks, which was configured using the CAPolicy.inf. The APP1 CRL must be updated weekly by default. To update the CRL, use the command:  Certutil –crl, which publishes the CRL to the locations that you specified in the CA Properties Extensions tab. | |

Top of Form



Did you find this helpful? YesNo

Not accurate

Not enough depth

Need more code examples



(1500 characters remaining)

Bottom of Form

Community Content[Add](http://technet.microsoft.com/en-us/library/community/add/hh831348.aspx)

[Annotations](http://technet.microsoft.com/en-us/library/community-edits.rss?topic=hh831348|en-us|WS.11)[FAQ](http://technet.microsoft.com/en-us/library/community-msdnwikifaq.aspx)

Seems I cannot edit comments to answer specifically, so this has two responses:

INET1 does not have a role in this lab, I mentioned that in a note at the start of the lab.  
I have no idea why the PowerShell cmd would fail with a network error. That does not even make sense. When I wrote and tested these instructions, I ran the commands directly on the systems that I was configuring. Are you perhaps trying to run the PowerShell cmdlet remotely? That is my only guess as to why it would fail. I am not the only person who tested this lab either. A few other people checked my work.

[History](http://technet.microsoft.com/en-us/library/community/history/hh831348.aspx?id=4)

http://i3.technet.microsoft.com/Areas/Global/Content/clear.gif

[http://i1.social.s-msft.com/profile/u/avatar.jpg?displayname=kurt+l+hudson&size=small](http://social.technet.microsoft.com/profile/kurt%20l%20hudson/)

* 9/7/2012
* [Kurt L Hudson](http://social.technet.microsoft.com/profile/kurt%20l%20hudson/)

[http://i1.social.s-msft.com/profile/u/avatar.jpg?displayname=kimwinters&size=small](http://social.technet.microsoft.com/profile/kimwinters/)

* 11/5/2012
* [kimwinters](http://social.technet.microsoft.com/profile/kimwinters/)

installing standalone CA with PS commands fails

*Install-AdcsCertificationAuthority –CAType StandaloneRootCA –CACommonName “ContosoRootCA” –KeyLength 2048 –HashAlgorithm SHA1 –CryptoProviderName “RSA#Microsoft Software Key Storage Provider”*

**This fails:**"Install-AdcsCertificationAuthority : Active Directory Certificate Services setup failed with the following error: The network location cannot be reached.

[History](http://technet.microsoft.com/en-us/library/community/history/hh831348.aspx?id=2)

http://i3.technet.microsoft.com/Areas/Global/Content/clear.gif

[http://i1.social.s-msft.com/profile/u/avatar.jpg?displayname=jeramy_t&size=small](http://social.technet.microsoft.com/profile/jeramy_t/)

* 7/30/2012
* [Jeramy\_T](http://social.technet.microsoft.com/profile/jeramy_t/)

[http://i1.social.s-msft.com/profile/u/avatar.jpg?displayname=kimwinters&size=small](http://social.technet.microsoft.com/profile/kimwinters/)

* 11/5/2012
* [kimwinters](http://social.technet.microsoft.com/profile/kimwinters/)

INET1

What is the role of INET1 in this lab

[History](http://technet.microsoft.com/en-us/library/community/history/hh831348.aspx?id=3)

http://i3.technet.microsoft.com/Areas/Global/Content/clear.gif

[http://i1.social.s-msft.com/profile/u/avatar.jpg?displayname=yogesh_eps&size=small](http://social.technet.microsoft.com/profile/yogesh_eps/)

* 8/24/2012
* [Yogesh\_Eps](http://social.technet.microsoft.com/profile/yogesh_eps/)

[http://i1.social.s-msft.com/profile/u/avatar.jpg?displayname=kimwinters&size=small](http://social.technet.microsoft.com/profile/kimwinters/)

* 11/5/2012
* [kimwinters](http://social.technet.microsoft.com/profile/kimwinters/)

Server Core installation tip

If you are installing a CA with server core, and do not have a Certification Authority console, you can simple type  
certutil -installcert   
  
to replicate step 34 from **To install the enterprise subordinate CA role**  
  
  
34. On APP1, in the Certification Authority console, right-click the **IssuingCA-APP1**, click **All Tasks**, and then click **Install CA Certificate**.  
35. In the **Select file to complete CA installation**, set the file type to **X.509 Certificate (\*.cer; \*.crt)** and then navigate to the removable media and select **APP1.corp.contoso.com\_IssuingCA-APP1.crt**. Click**Open**.

[History](http://technet.microsoft.com/en-us/library/community/history/hh831348.aspx?id=5)

http://i3.technet.microsoft.com/Areas/Global/Content/clear.gif

[http://i1.social.s-msft.com/profile/u/avatar.jpg?displayname=hackajar&size=small](http://social.technet.microsoft.com/profile/hackajar/)

* 9/13/2012
* [hackajar](http://social.technet.microsoft.com/profile/hackajar/)

[http://i1.social.s-msft.com/profile/u/avatar.jpg?displayname=kimwinters&size=small](http://social.technet.microsoft.com/profile/kimwinters/)

* 11/5/2012
* [kimwinters](http://social.technet.microsoft.com/profile/kimwinters/)

FILE: moniker

Has support for the file:// moniker been re-added in Windows 8? I can appreciate this is a lab environment but I was on the understanding that the file:// moniker has been removed in Windows Server 2008 R2.  
  
--------------------------------------------------  
Answer by Kurt Hudson, author of this lab:  
You can use the file:// moniker in both Windows Server 2008 R2 and Windows Server 2012. An update to this lab (since you wrote the comment) shows that moniker in use.